



Seguridad Digital:

El reto del riesgo cero.

Editorial

El contexto tecnológico actual exige un nuevo paradigma de seguridad enfocado a monitorizar y analizar toda la información disponible para identificar y prevenir cualquier ataque cibernético malicioso que las organizaciones puedan sufrir.

Es necesario impulsar una visión integradora para garantizar la seguridad y el progreso de la infraestructura de las compañías de cara a obtener una mejor comunicación entre sus diferentes entornos, primando la seguridad por encima de todo.

Se hace imprescindible que organizaciones y entidades desarrollen de forma coherente y estructurada las acciones de prevención, detección, respuesta y recuperación frente a las Ciberamenazas, así como también el desarrollo de un plan estratégico de Ciberseguridad acorde a cada organización o infraestructura.

Dichas acciones deben llevarse a cabo sobre la base de la coordinación, cooperación y concienciación entre las diferentes áreas involucradas, ya que solo de esta forma podrán afrontarse las nuevas amenazas de seguridad digitales surgidas en los últimos años, y cuya evolución y potencia es exponencial.

Rafael Conde del Pozo
(Digital & Innovation Director, Vector ITC).



Índice

01 **6 – 11**

Situación actual de la Ciberseguridad.

02 **12 – 31**

Amenazas y tipos de ataques.

03 **32 – 55**

Tipología de ataques de seguridad.

04 **56 – 61**

¿Cómo proteger los datos?

05 **62 – 66**

Nuestras Conclusiones.





Situación actual de la Ciberseguridad.

01

En un contexto empresarial caracterizado por la apuesta estratégica por la digitalización, la protección de los activos digitales adquiere una relevancia esencial. Los ciberataques y las fugas de datos tienen mayor capacidad que nunca para afectar a la actividad de las compañías, no solo por lo que se refiere al riesgo directo de los sistemas informáticos, sino también por la problemática reputacional que genera en cualquier empresa una fuga masiva de datos de sus usuarios.

El año 2018 tuvo como elemento central la privacidad de los datos, con el Reglamento General de Protección de Datos (GDPR) impulsado por la Unión Europea, que se sitúa a la vanguardia global del entorno regulatorio digital. Este año se han popularizado los softwares de criptomonedas ilegales, que se han convertido en una de las principales amenazas para los ordenadores de usuarios y empresas, y que ocupan hoy un lugar destacado en el escenario de amenazas cibernéticas, de un modo parecido al que lo hiciera el Ransomware en el año 2017.

Sin lugar a dudas, el protagonismo del Cryptojacking, la técnica ilegal de minado de criptomonedas sin conocimiento ni autorización del usuario puede ser disputado tan solo por los riesgos derivados de los hogares inteligentes y los asistentes de voz, tendencia con cada vez mayor implantación entre particulares y empresas, y que pueden convertirse a corto plazo en el principal foco de las ciberamenazas. **La protección de los dispositivos IoT requiere de soluciones de seguridad adaptadas** o incluso específicamente diseñadas para este tipo de dispositivos. Innovaciones como los honeypots ya avanzan en esta dirección.





Por supuesto, también **la adopción de la nube es un fenómeno crítico, pues plantea nuevas plataformas de gestión de infraestructura y datos** de complejidad mucho mayor a las tradicionales, con entornos híbridos y SaaS que, si bien se basan en sistemas más seguros, también demandan una especialización mucho mayor de los técnicos que los gestionan con tal de garantizar la protección de los datos.

No obstante, la popularización de nuevas vías de ataque no relega en ningún caso a las tradicionales, y es que el correo electrónico continúa siendo el principal canal de entrada de Malware, con más del 80% de las amenazas explotando esta vía. La sofisticación de este tipo de ataques es cada día mayor, pese a lo clásico del canal, y la principal respuesta que deben tener las empresas no es otra que la formación del personal. La concienciación de los empleados es un punto crítico que ni siquiera el más avanzado de los sistemas de Ciberseguridad puede omitir.

Por otra parte, **el entorno de las empresas es cada vez más abierto y difuso, por la creciente integración de sistemas con terceras partes**, lo que está revolucionando la seguridad perimetral. Por primera vez, el reto de una organización no es tan solo asegurar su perímetro con las herramientas más avanzadas, sino también asegurar que los sistemas de sus partner cuentan con una protección análoga. La monitorización continua, los privilegios mínimos, el cifrado o la ofuscación son algunas de las técnicas que las empresas más avanzadas están implantando para garantizar la confiabilidad de sus sistemas en un contexto de perímetro no medible.



Los retos no tienen un carácter exclusivamente tecnológico. **La formación del personal y la captación de talento son asignaturas pendientes** de las empresas, al mismo nivel que el desarrollo de sistemas preventivos más avanzados. Se estima que se requerirán 1,8 millones de profesionales de la Ciberseguridad a nivel mundial en 2022.

Los perfiles que se demandan son muy variados, desde CISOs expertos en gobierno de la Ciberseguridad, pasando por arquitectos especializados en diseño de arquitecturas de red o pentesters experimentados en análisis forense, hasta consultores de privacidad que guíen la adaptación al nuevo entorno GDPR.

Los nuevos retos en materia de Ciberseguridad también generan grandes oportunidades de negocio, en particular para las aseguradoras. Teniendo en cuenta que las técnicas de detección y respuesta son difícilmente infalibles, son cada vez más populares los ciberseguros para empresas, con tal de prevenir el impacto económico y reputacional que un hipotético ataque podría generar en cualquier organización. Para muchas empresas, el valor de sus datos es muy superior al de sus infraestructuras físicas, por lo que no resulta extraño que, si existe un amplio consenso en torno a la necesidad de asegurar sus edificios, almacenes u oficinas, cada vez sean más las compañías que demanden asegurar sus activos digitales.

Mientras los ciberataques continúan sofisticándose, también lo hacen los sistemas de protección. Un buen ejemplo de ello son las soluciones de Digital Risk Protection (DRP), que permiten a las empresas proteger su identidad de marca y la de sus ejecutivos o, en general, de todos los activos digitales fuera de su perímetro. El objetivo de estas soluciones es monitorizar los activos para recuperarse rápidamente de los ataques y prevenir el riesgo reputacional. Asimismo, los servicios de Managed Detection and Response (MDR) proporcionan una monitorización en tiempo real de toda la red, detectan comportamientos anómalos y ofrecen una respuesta ágil para prevenir el ataque antes de que realice su potencial malicioso.



Pero si alguna tecnología reinará el desarrollo tecnológico de la Ciberseguridad, esta será el Machine Learning. Los algoritmos pueden identificar amenazas de un modo mucho más eficiente que los sistemas tradicionales basados en firmas y heurística, y al basarse en técnicas de aprendizaje automático, las herramientas son cada vez más confiables y adquieren un conocimiento mayor de las potenciales amenazas. Sin embargo, también los cibercriminales están utilizando esta tecnología para crear ataques automatizados mucho más eficaces.

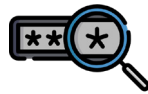
Junto a la panorámica general, existen muchas tendencias que determinarán el campo de la Ciberseguridad a corto plazo:



Popularización del Cryptojacking, que pone al servicio de los ciberdelincuentes la capacidad de computación de particulares y empresas, generando ingresos millonarios. Asimismo, pueden servir como puerta de entrada para otros tipos de Malware, o propagarse a sí mismos a través de la red.



Vulnerabilidad de los sistemas de Inteligencia Artificial (IA), cuya adopción empresarial es cada vez mayor, y que permite la toma automática de decisiones clave. Por ello, el potencial daño que podría generar en una compañía la vulneración de estos sistemas es enorme.



Preocupación creciente por la privacidad de los datos personales, con un entorno regulatorio global especialmente activo, como muestra la GDPR. La adaptación de las empresas a este nuevo marco es un reto que todavía hoy está pendiente para muchas pequeñas y medianas empresas.



Reducción del número de ataques basados en Ransomware, ante su índice cada vez mayor de detección preventiva, y la popularización de nuevas formas de malware como los Cryptominers ilegales.



Miniaturización de los ciberriesgos, que no afectarán únicamente a los ordenadores o grandes infraestructuras de datos, sino también a dispositivos móviles, routers, dispositivos IoT o tablets. En este sentido, ha aumentado considerablemente el número de aplicaciones maliciosas capaces de robar credenciales a los usuarios o introducir Cryptominers ocultos.



Continuación del espionaje ilegal por parte de grandes empresas, incorporando por defecto software no autorizado por el usuario en sus dispositivos, que permite el acceso a la información almacenada, la cámara o el micrófono, sin conocimiento del propietario.

En definitiva, la imparable digitalización de las empresas no es solo una gran oportunidad, sino que entraña importantes riesgos, dado que los activos digitales son cada vez más parte esencial del patrimonio de cualquier organización, y que la adopción de nuevos sistemas y herramientas como el almacenamiento en la nube, el IoT o la IA, generan también nuevas ventanas de oportunidad para los ciberdelincuentes y requieren de sistemas de protección más sofisticados, y de expertos capaces de gobernarlos.



Amenazas y tipos de ataques.

02

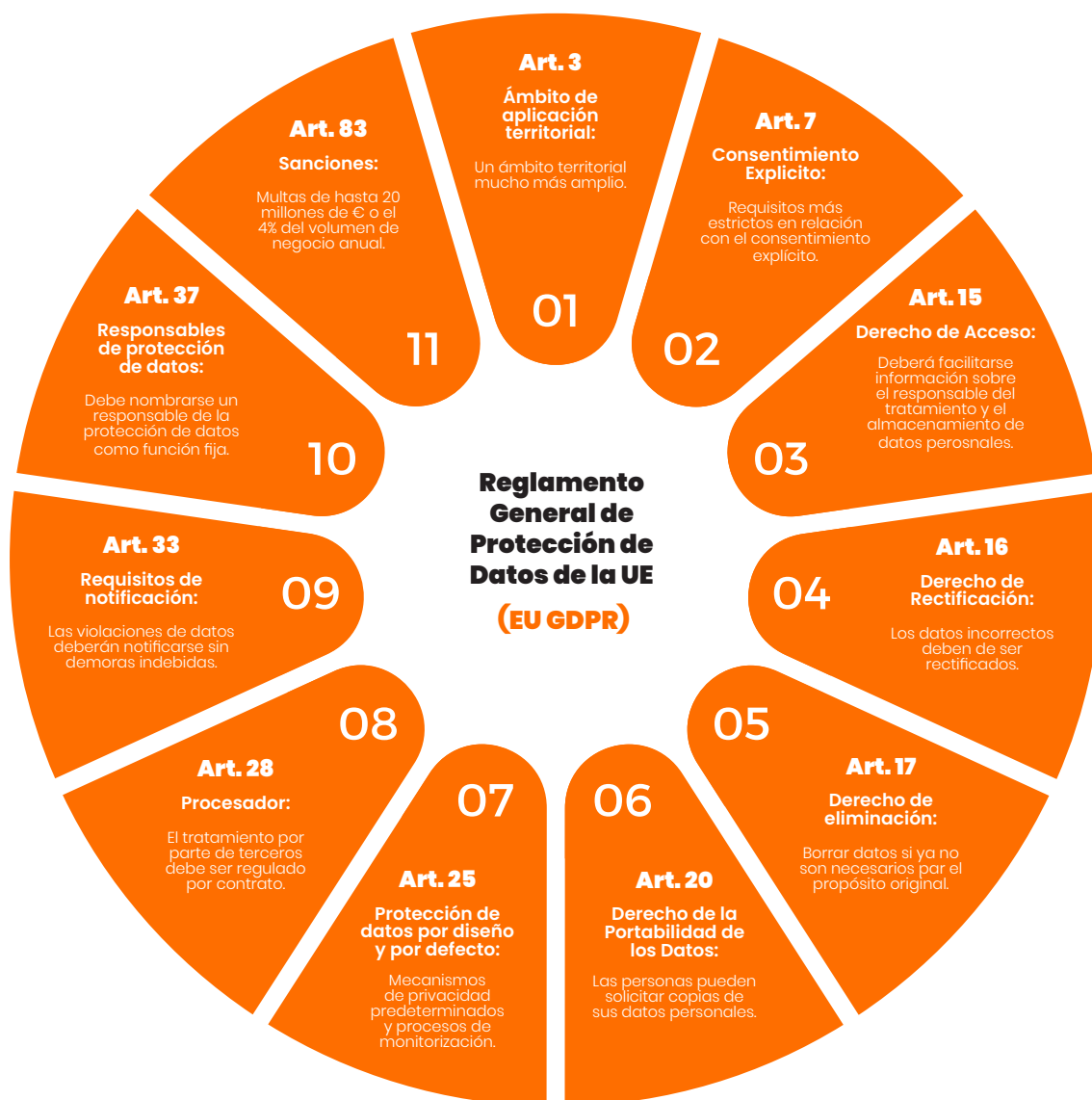


PROTECCIÓN DE LOS DATOS Y PRIVACIDAD.

La preocupación sobre la privacidad de los datos alcanza máximos históricos. Más del 40% de la población mundial siente que carece de control sobre sus datos personales, y un tercio de los padres no saben cómo explicar los riesgos de seguridad online a sus hijos. Gran parte de estas preocupaciones vienen dadas por la violación de datos sufrida por grandes compañías como Facebook, Panera Bread o Sacramento Bee. Y si bien el robo de identidad es una preocupación común, no es el único riesgo que enfrentan los datos personales.

Ante esta situación, en mayo de 2018, la Unión Europea promulgó el **Reglamento General de Protección de Datos (GDPR)**, la ley de privacidad de datos más dura y compleja hasta la fecha, que establece a las empresas una serie de obligaciones relacionadas con la privacidad y posibles multas por incumplimiento.

Antes del GDPR, las empresas no estaban obligadas a mostrar exactamente qué datos habían recopilado sobre una persona en particular. Ahora, según el artículo 6.1.a de dicho reglamento, deben obtener el consentimiento explícito de las personas antes de almacenar datos personales o procesarlos para un propósito específico.



A su vez, los usuarios tienen **derecho a acceder, rectificar y eliminar datos personales** a petición, y pueden presentar una queja si sienten que sus datos están siendo mal utilizados. De este modo, la legislación faculta a las personas al tiempo que crea una serie de nuevas obligaciones para las empresas. El incumplimiento del GDPR puede dar lugar a importantes multas, que pueden llegar a los 20 millones de dólares o el 4% de los ingresos anuales, dependiendo de la cantidad que sea mayor.

Esta nueva tendencia sobre la privacidad de los datos cambia drásticamente la forma en que las entidades privadas recopilan y procesan la información del consumidor.

La nueva legislación está ampliando la definición de datos personales para incluir información identificable que se recopila automáticamente, mientras que antes este tipo de datos no tenían tal consideración.

Se deben desarrollar las herramientas necesarias para garantizar que los **datos personales se recopilen, almacenen y procesen de manera transparente**. En este contexto, las empresas están apostando por soluciones de gestión de datos automatizadas, basadas en IA, para implementar políticas sólidas de privacidad de datos sin sacrificar productividad o agilidad operacional.

CIBERSEGURIDAD MÓVIL. APPS MÓVILES MALICIOSAS:

La adopción de dispositivos y comunicaciones móviles, tanto en el ámbito personal como profesional, ha alcanzado un nivel de madurez y estabilidad durante la última década en el que resulta difícil imaginar la realización de las actividades cotidianas sin hacer uso de estos. La utilización permanente y extensiva de estas tecnologías confirma a los **dispositivos móviles como uno de los objetivos principales** de las ciberamenazas para el año 2020.

La seguridad móvil forma parte de una de las principales preocupaciones de las empresas, y es que los trabajadores acceden rutinariamente a datos corporativos desde teléfonos inteligentes. Eso significa que **no es suficiente con proteger las infraestructuras de la empresa**, en base a un esquema cerrado de seguridad perimetral, sino que el carácter abierto del entorno impone un nuevo concepto de Ciberseguridad que incluye a los dispositivos móviles.



MALWARE MÓVIL

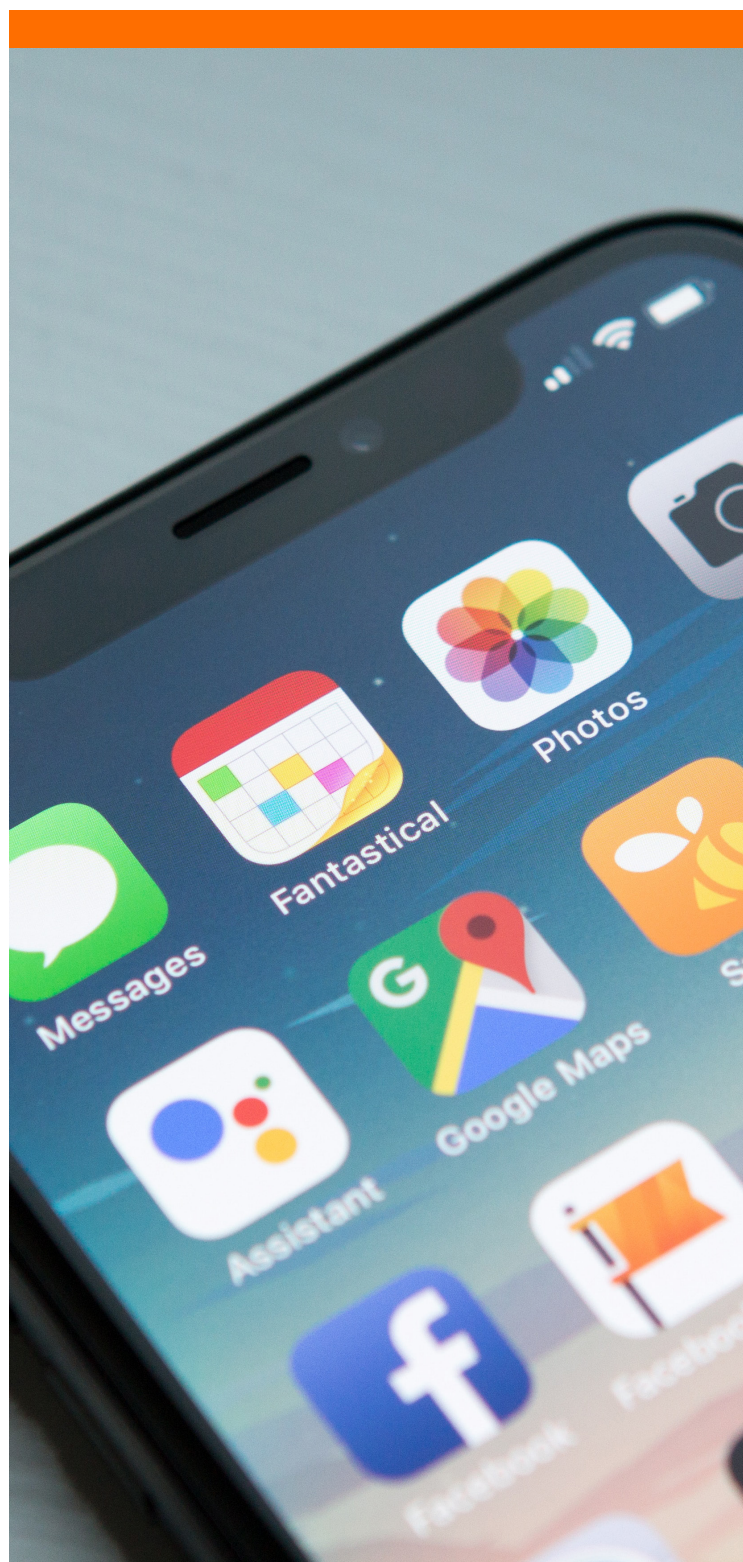
Existe un crecimiento global de Malware móvil. Destacan algunas campañas como las de Apps maliciosas que proporcionan una ventana de navegación web (WebView) para ataques de Phishing, principalmente contra Bancos online, evitando así la detección por parte del usuario, al ser distribuidas a través de Google Play Store.

Otros Malware se han introducido en Apps legítimas de fabricantes de dispositivos móviles, como Sound Recorder, tras vulnerar el proceso de desarrollo de esta compañía o de uno de sus partners, logrando así la distribución de Malware móvil preinstalado.

Asimismo, se ha identificado un **incremento en la distribución de código para minar Criptomonedas** dentro de otras Apps, como juegos o utilidades. Esta técnica, llamada Cryptojacking, es un ataque que los criminales lanzan para "secuestrar" parte de la capacidad de proceso del teléfono y dedicarla a labores de minería de Criptomonedas, sin que el dueño del terminal lo perciba. El código puede ser ejecutado cuando la App está siendo utilizada y cuando no, y tiene un impacto directo en el consumo de batería del dispositivo. Dado que este código no es inherentemente malicioso, es habitual que se permita su distribución a través de Google Play Store.

Además, el fraude a través de anuncios constituye uno de los negocios más lucrativos actualmente, y su distribución a través de Apps móviles juega un papel muy relevante y creciente. El coste estimado de anuncios fraudulentos (sobre los que supuestamente ha pulsado el usuario) a nivel global (no sólo móvil) es de 19.000 millones de dólares al año.

Una tendencia que está popularizándose a gran velocidad es la asociada a la **existencia de Malware móvil preinstalado en algunos dispositivos** ya que el Malware forma parte, o es en sí mismo, una App del sistema que no puede ser desinstalada, aunque sí deshabilitada o desactivada en algunos casos.





Un primer ejemplo fue Adups, una App preinstalada en dispositivos de fabricantes como BLU, que no podía ser siquiera desactivada desde la interfaz de usuario. Otro ejemplo de este tipo es Riskware, descubierto en el modelo THL T9 Pro, embebido en la App System UI. También Monitor, descubierto en el modelo UTOK Q55, centrado en la recolección y envío de información sensible del usuario.

Estas infecciones, donde el código malicioso se ha embebido y, por tanto, ha troyanizado Apps críticas de sistema, son complejas de remediar. En algunos casos se podría sustituir la App afectada por una versión legítima de la misma para la misma versión de Android.

Complementariamente, dentro de las amenazas del Malware móvil más comunes y utilizadas, sigue estando el **Ransomware móvil, bloqueando el dispositivo o amenazando al usuario**; Adware para la obtención de beneficios económicos a través de anuncios y que en algunos casos se ha distribuido a través de Google Play Store. El Ransomware ataca directamente a la información almacenada en el terminal, como fotos, vídeos, etc., cifrando dicha información a la espera de que el usuario pague un rescate para recuperarla.

En muchos casos, el Malware **intenta obtener permisos como administrador del dispositivo** e implementa diferentes medidas para no perderlos una vez obtenidos, como ocultarse o dificultar su desinstalación.

También se están detectando ataques a móviles que consisten en la duplicación de la tarjeta SIM tras la captura de algunos datos confidenciales. En este caso, los ciberdelincuentes tratan de obtener acceso a la SIM porque el móvil es la herramienta que hace posible el doble factor de autenticación (por ejemplo, recibiendo el código con el que se validan las compras online a partir de cierta cantidad de dinero). De esta manera, los delincuentes pueden tener acceso a operaciones bancarias, cambios de contraseña en las redes sociales o en servicios en la nube donde los usuarios (y también las empresas) guardan su información más preciada.

PHISHING

En todo caso, y como ocurre en el mundo PC, conviene recordar que los ataques de Phishing siguen siendo los que mayor impacto tienen entre los usuarios de dispositivos móviles. El envío de correos que incorporan un enlace fraudulento es la vía más usada por los delincuentes para obtener contraseñas y accesos a servicios de las víctimas. Precisamente, uno de los accesos más codiciados es el de las aplicaciones de gestión de claves que almacenan en un mismo repositorio todas las contraseñas del usuario.

También están ganando peso los ataques de Phishing a través de SMS. Este tipo de mensajería se utiliza cada vez como canal seguro para la autenticación de dos factores o la recuperación de contraseñas. Así que no es de extrañar que haya crecido el interés de los hackers por explotar las vulnerabilidades de este canal.

DAÑO REPUTACIONAL

Las compañías deben definir una estrategia clara de Ciberseguridad. En el caso de ataques dirigidos a empresas, los hackers muchas veces no buscan la obtención de datos de manera directa, pero sí dañar la reputación de la compañía o el bloqueo de infraestructuras y servidores.

Los ataques de ciberespionaje a través del móvil mantienen una tendencia alcista, y es que las herramientas de monitorización comercializadas en el mercado para realizar el seguimiento de las comunicaciones del terminal ponen de manifiesto la relativa facilidad con la que este tipo de ataques logran acceder a los dispositivos.

También se están haciendo habituales los puntos de acceso Wi-Fi falsos o de “gemelo maligno”. En este caso, los ciberdelincuentes utilizan el mismo SSID (parámetro que identifica a la red inalámbrica) que el punto de acceso original para que el usuario se conecte erróneamente a ellos y así poder robarle la información.

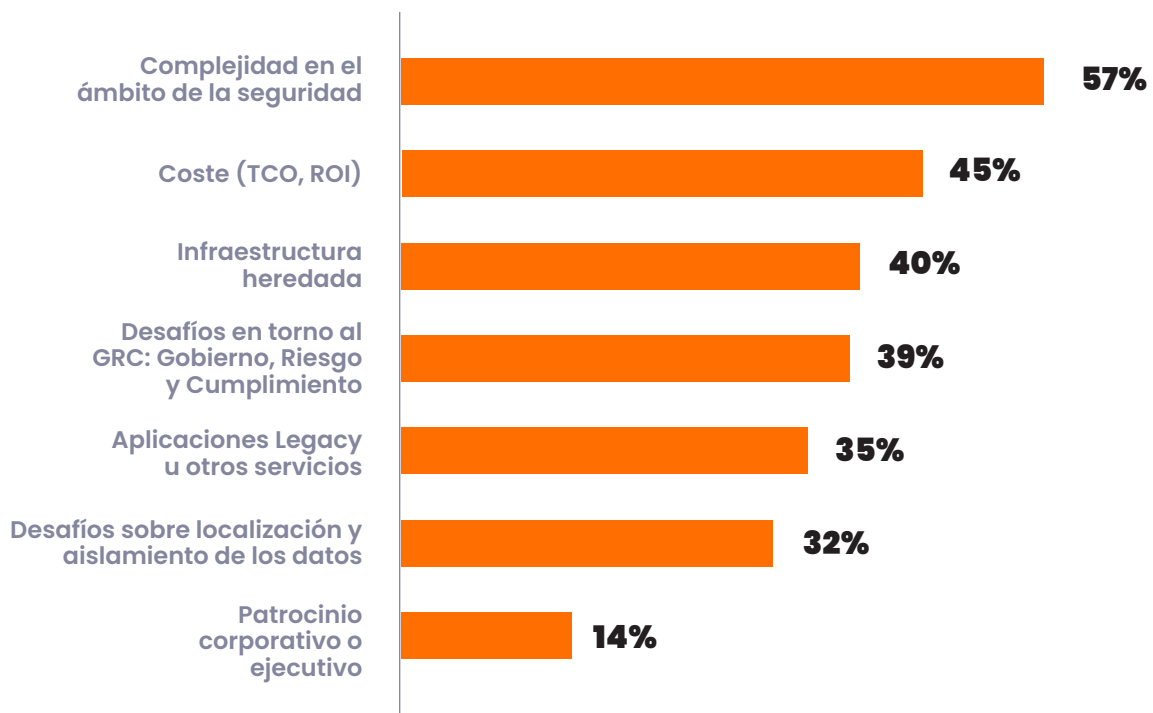
A esto se suma que cada vez más las organizaciones apuestan por el BYOD (Bring Your Own Device), permitiendo que los empleados hagan uso de sus propios dispositivos personales en el lugar de trabajo, en muchos casos sin implementar las herramientas de seguridad ni recibir la formación necesarias. Y esto, sin duda, supone una amenaza importante para la seguridad de las empresas y, por ende, para su información corporativa.



CONFIANZA EN LA NUBE. SEGURIDAD EN CLOUD COMPUTING:

En estos momentos, hay miles de organizaciones que utilizan herramientas que dependen de la nube para almacenar archivos clave de los clientes. Y si bien la adopción de la nube presenta ventajas estratégicas para las compañías, no está exenta de desafíos: la seguridad sigue siendo la principal preocupación, seguida de la gestión y el seguimiento del gasto en la nube, y la falta de habilidades.

Los mayores retos de la adopción de la nube:



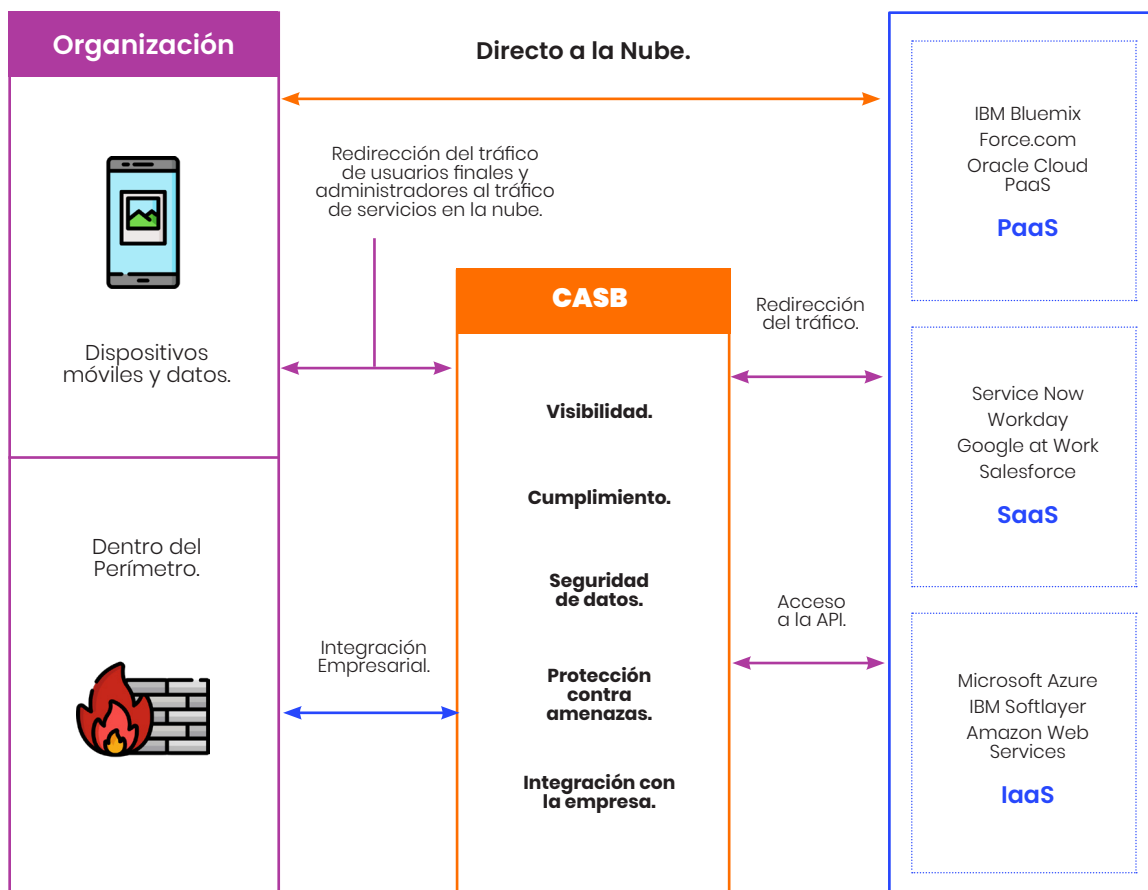
A menudo, los profesionales del sector hablan sobre la implementación de la Confianza Cero para un entorno nativo de la nube como solución ante las dudas que surgen sobre la seguridad Cloud. Esta falta de confianza puede manifestarse de varias maneras.

OBSTÁCULOS A SUPERAR

Asumir que la información privada está almacenada en un dispositivo ajeno puede desencadenar una preocupación sobre la privacidad de esos datos. **La mayoría de los servicios en la nube ofrecen un nivel básico de cifrado y protección para los datos que almacenan.** Además, garantizan la protección física del centro de datos con paredes gruesas y resistentes al fuego, y cifran los datos que almacenan para mitigar el riesgo de violación. Pero a pesar de eso, incluso el servicio en la nube más seguro podría verse comprometido si la autorización del usuario se ve comprometida.

Por otra parte, la necesidad de estar conectado a Internet supone un obstáculo en la confianza de las empresas hacia los sistemas Cloud. El riesgo de pérdida temporal de la conexión a la red genera intranquilidad, al no poder contar con el control absoluto del funcionamiento. No obstante, cada vez son más las aplicaciones que también ofrecen sus servicios offline.

Además, si bien la computación en la nube no es inherentemente insegura, requiere un enfoque de seguridad diferente. Los datos son valiosos para los ciberdelincuentes, pero no todos los datos se crean de la misma manera. Por ello, las organizaciones deben, en primer lugar, clasificar sus tipos de datos, para luego invertir en herramientas de defensa sólidas para almacenarlos y protegerlos adecuadamente. Esta necesidad ha dado lugar a un nicho de mercado, las **herramientas de seguridad cibernética que desde entonces se han clasificado como Cloud Access Security Brokers (CASB).**



PRIORIDAD DE SEGURIDAD

Las compañías deben cumplir con los estándares de seguridad cibernética que garantizan la integridad de los datos de los usuarios. Así, por una parte, el **acceso a la aplicación debe estar dotado de un certificado SSL** (Secure Sockets Layer) donde se indique la identidad de los propietarios del sitio.

También se recomienda que la nube tenga autenticación multifactorial, lo que significa que después de las credenciales de usuario y contraseña, debe haber una segunda o tercera fase que verifiquen el acceso de forma segura.

Por otra parte, los firewalls y los grupos de usuarios seguros también son claves para trabajar de forma segura con un servicio en la nube. Se pueden crear grupos de usuarios seguros y discriminar el acceso a los recursos según el nivel de privilegios.

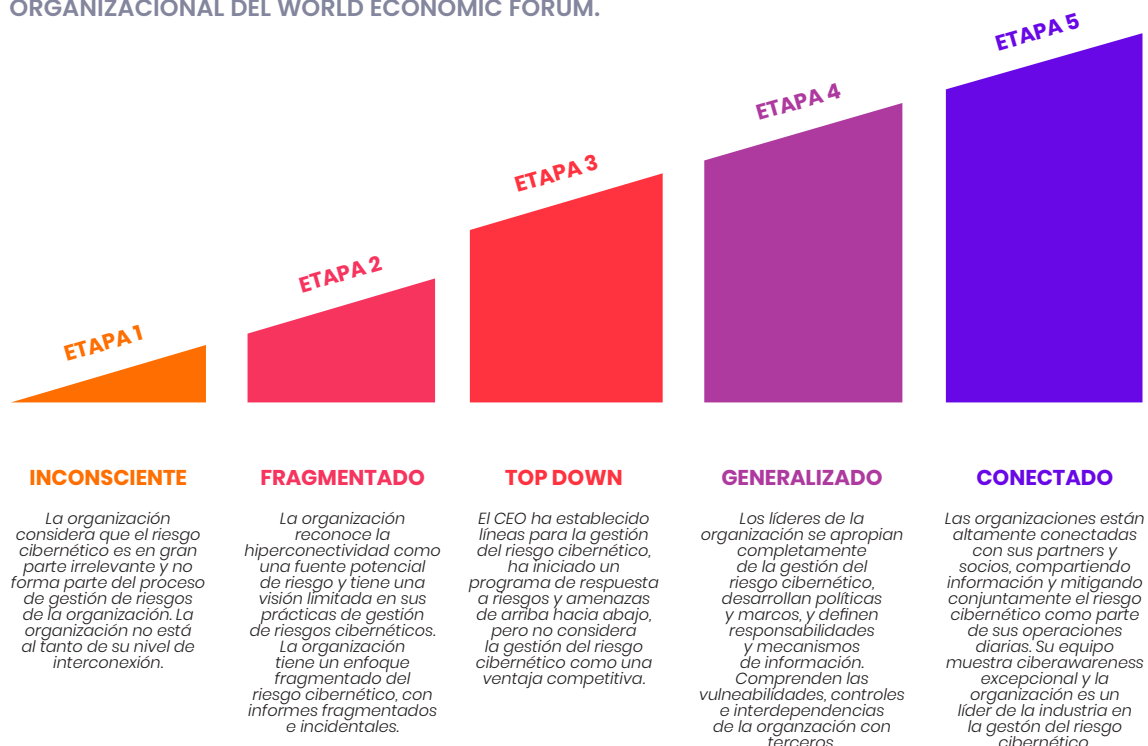
El cifrado también es importante para evitar la lectura de datos por parte de terceros. Algunos servicios en la nube lo integran. Hay aplicaciones que mantienen la privacidad de los archivos con cifrado de punto final como Dropbox, Google Drive o OneDrive, entre otros.



INCLINACIÓN HACIA EL MODELO DE CIBER-RESILIENCIA:

En la actualidad, el ánimo de lucro de los ciberdelincuentes y la rápida evolución de los malwares hacen cada vez más difícil garantizar la seguridad de las empresas, independientemente de su tamaño y sector, surgiendo así el concepto de Ciber-Resiliencia. Ser **ciber-resiliente ayuda a las empresas a concienciarse y a adquirir una actitud proactiva frente a vulnerabilidades, riesgos y ataques**, es decir, es la capacidad de una empresa de prevenir, detectar, contener, adaptarse y recuperarse con sus funciones y su trabajo en situaciones de riesgo. Cómo actuar y cómo gestionar la situación de forma eficiente afectando el mínimo posible al desempeño general de la empresa.

MODELO DE MADUREZ DE LA CIBER-RESILIENCIA ORGANIZACIONAL DEL WORLD ECONOMIC FORUM.



Debemos asumir que es imposible frenar al 100% los ataques cibernéticos. Adoptar una actitud resiliente frente a las vulnerabilidades es imprescindible para ser capaz de **gestionar el riesgo existente y superarlo con un mínimo impacto** para la organización. En comparación con las defensas tradicionales que ya no sirven una vez ocurrido el incidente, la Ciber-Resiliencia posibilita una vigilancia constante en toda la organización.

El marco de Ciber-Resiliencia está compuesto por cinco elementos:



Identificar o Evaluar:
correlacionar activos y procesos críticos, evaluar el riesgo y afrontarlo.



Proteger:
primera línea tradicional de los mecanismos de seguridad defensivos.



Detectar o Monitorizar:
análisis de la seguridad.

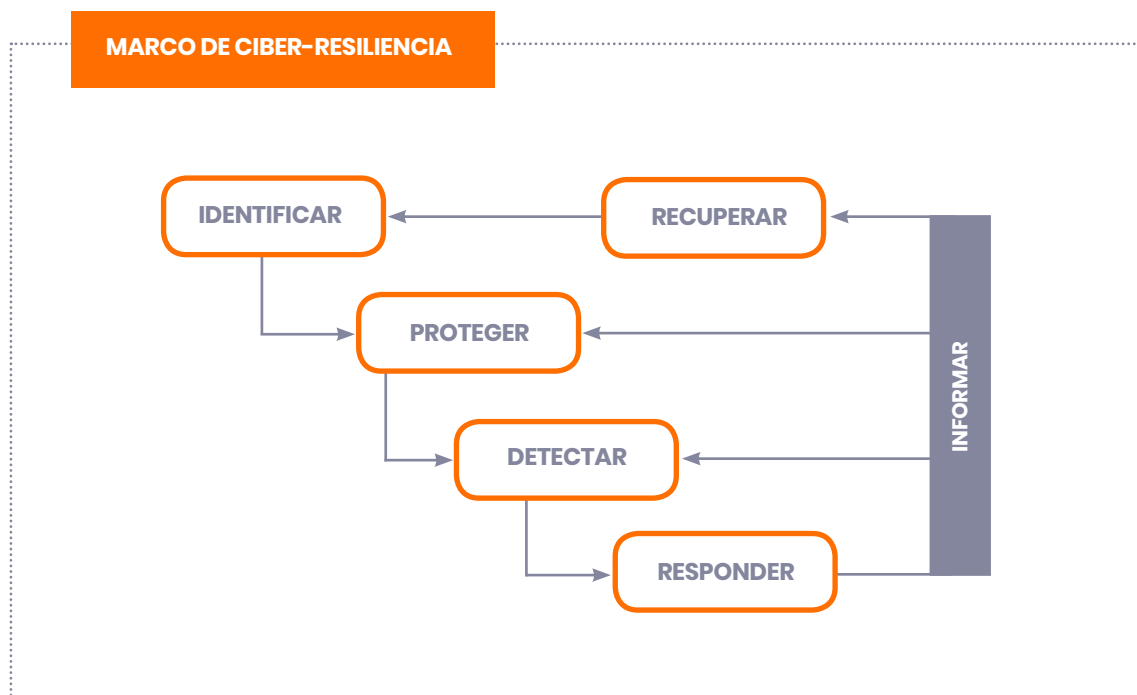


Responder o Solucionar:
respuesta ante una brecha de seguridad o fallo.



Restaurar o Recuperar:
mecanismos coordinados de restauración.

La principal ventaja del marco de Ciber-Resiliencia es que está dirigido al **negocio**. Tradicionalmente, la seguridad funcionaba como un componente adicional del negocio. La Ciber-Resiliencia integra la seguridad dentro de la empresa en sí, lo que permite que los cinco componentes estén presentes en todas las áreas del negocio.



La seguridad es compleja, y sencillamente no hay manera de probar que un entorno sea seguro. Los atacantes siguen usando métodos innovadores para irrumpir en las organizaciones, recurriendo a cualquier táctica que sea necesaria para lanzar un ataque con éxito. Lo mejor que puede esperar una organización es contar con una **infraestructura reforzada, funciones y procesos auditables, usuarios cualificados, personal de seguridad destacado y procesos de monitorización continua**.

LA TECNOLOGÍA COMO CLAVE

Aunque el marco de Ciber-Resiliencia pueda parecer intuitivo, debe implementarse por medio de una cuidadosa selección de tecnologías. No existe un único producto que pueda crear un entorno Ciber-Resiliente, sino que existen tecnologías clave que una organización puede emplear para afrontar una posible interrupción en las actividades como consecuencia de un ciberataque. Las tecnologías que se describen a continuación son fundamentales para que las organizaciones puedan crear un entorno resiliente:

Lineamientos básicos de seguridad:

Los lineamientos básicos de Ciberseguridad son un conjunto de políticas, resultados, actividades, prácticas y controles, **destinados a ayudar a gestionar el riesgo de seguridad digital**. Algunos ejemplos a nivel internacional son la Guía de controles ISO/IEC 27002; Center For Internet Security, CIS; Guías de controles del National Institute of Standards and Technology, NIST; Guía de controles críticos de seguridad de Sans Institute.

Protección perimetral en forma de copia a prueba de fallos contra la propagación de Malware:

La protección del perímetro es una medida de seguridad que consiste en separar sistemas o redes de otros sistemas o redes, por medios físicos o virtuales. Las empresas, por ejemplo, pueden optar por **aislar completamente las redes o sistemas que contienen datos altamente sensibles de la red operativa** que se utiliza todos los días. En la actualidad, la mejor práctica consiste en crear una copia de protección perimetral de los datos críticos a fin de mitigar la exposición externa, proteger a la organización de interrupciones en sus operaciones y evitar costes innecesarios.





WORM para evitar que los datos se corrompan o se borren:

El éxito actual de los ataques de Ransomware, como NotPetya, han puesto de manifiesto la necesidad de contar con una protección más fuerte contra la corrupción o el borrado de datos. **Las organizaciones deben contar con tecnologías que les garanticen datos inalterables.** Las tecnologías de almacenamiento inmutables (WORM, por sus siglas en inglés) pueden responder a esta necesidad, al permitir que las empresas conserven la integridad de sus datos y mantengan una resiliencia empresarial contra lo que han sido algunos de los ataques más paralizantes de los últimos tiempos. Existen muchas formas de tecnología WORM en la capa de software y en la capa de hardware, y ambas sirven para garantizar que los datos no sean manipulados.

Copias de momentos determinados y verificación de datos eficientes para identificar rápidamente los datos recuperables:

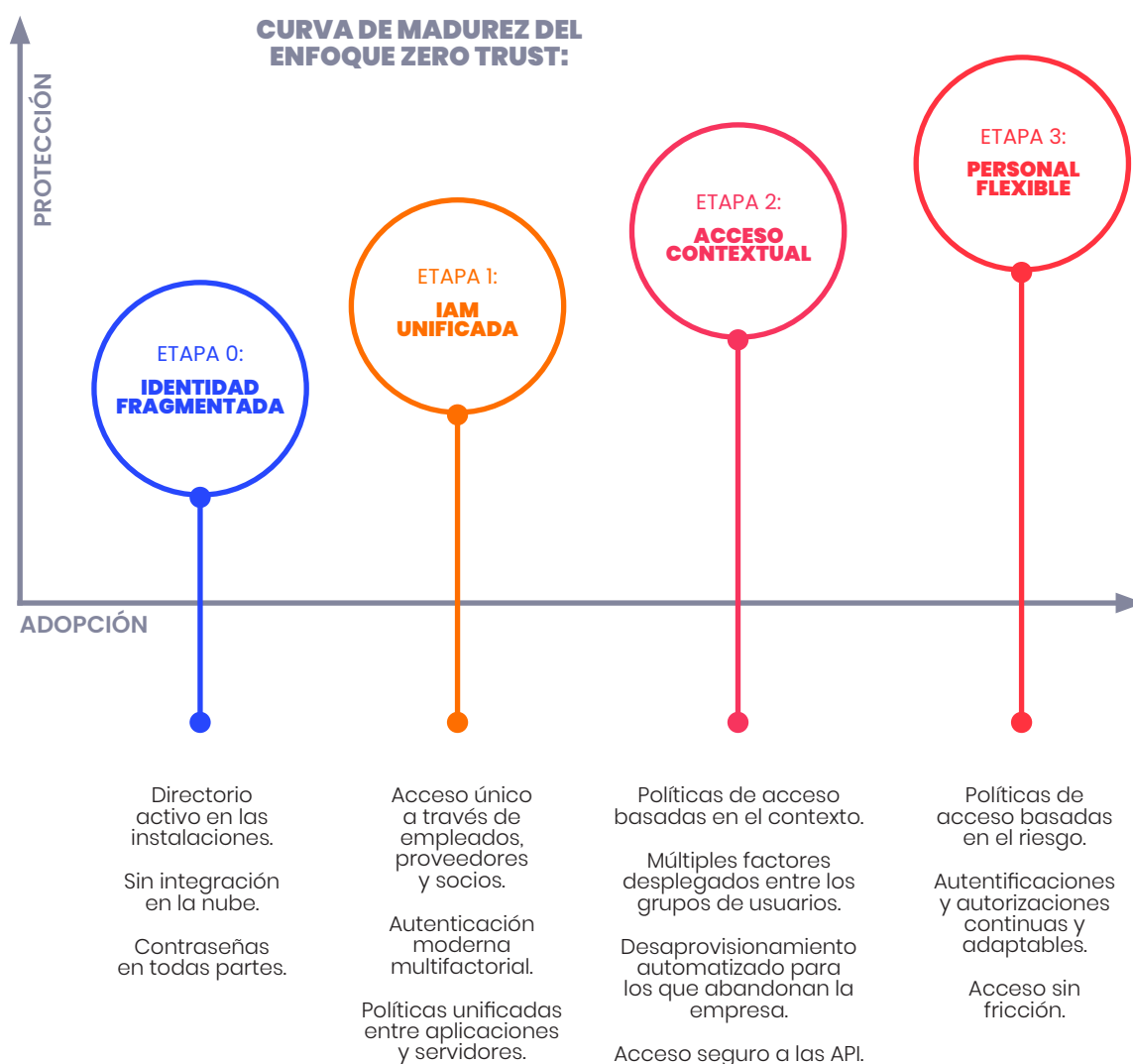
Una vez ocurrido el ataque, las organizaciones necesitan una manera de validar y restaurar rápidamente una copia válida de los datos. Por este motivo, se necesita una **tecnología de instantáneas (de momentos determinados) muy eficiente** para conservar múltiples copias de los datos. También es necesario realizar una verificación constante de esas copias para identificar de manera proactiva posibles infecciones y tomar medidas correctivas. El objetivo en cualquier caso es identificar rápidamente una copia de datos válida para el proceso de restauración.

Computación en la Nube:

La seguridad, elemento transversal en la computación Cloud, comprende desde la seguridad física hasta la seguridad digital, constituyéndose en un factor de competitividad, confianza y resiliencia de las organizaciones que hacen uso de este tipo de infraestructuras. La confianza de la computación en la nube está centrada en las siguientes condiciones: **seguridad, control y privacidad, cumplimiento de estándares y transparencia.** Dada la pluralidad y singularidad de las organizaciones, no existe una solución única Cloud, por lo que debe explorarse el uso de un modelo de inmersión completa o un modelo híbrido.

ADOPCIÓN DEL ENFOQUE DE CONFIANZA CERO:

El término Confianza Cero, también conocido como Zero Trust, es un modelo de Ciberseguridad con una premisa muy simple: eliminar el concepto de “confianza” de la red. Lo que **significa que ninguna comunicación, sistema, usuario o máquina puede acceder a ninguna parte de la red sin inspección y validación.**



Para implementar un modelo de Confianza Cero centrado en la red que haga hincapié en los comportamientos y políticas, los equipos de seguridad y operaciones deben **centrarse en dos conceptos clave:**



La seguridad deberá integrarse en las cargas de trabajo, y deberá moverse con las instancias y los datos a medida que migran entre los entornos de nube interna y pública.



El comportamiento real de las aplicaciones y servicios que se ejecutan en cada sistema deberá comprenderse mucho mejor. Por otro lado, las relaciones entre los sistemas y las aplicaciones **necesitarán un escrutinio más intenso que nunca para facilitar un modelo de operaciones altamente restringido** y sin confianza.

Cuando se cumple estrictamente, un modelo de Ciberseguridad Zero Trust puede ayudar a prevenir violaciones de datos. En estos momentos, muchas organizaciones están reinventando sus sistemas de Ciberseguridad fuera de los parámetros tradicionales y redefiniendo sus prácticas.



INTERPRETACIONES ERRÓNEAS

A pesar de los evidentes beneficios, existen varias situaciones que pueden dar pie a una **interpretación errónea al implementar una estrategia de seguridad** basada en el Zero Trust.

El camino hacia el Zero Trust comienza con la integridad de datos:

Las últimas investigaciones estiman que el 80% de las violaciones de datos son causadas por el mal uso de credenciales privilegiadas. Las credenciales privilegiadas brindan un mayor alcance para robar datos que las cuentas individuales, por lo que solo se necesita una credencial comprometida para impactar a millones de personas y causar una gran cantidad de daños. Por ello es importante **priorizar la administración de acceso privilegiado (PAM) en cualquier lista de proyectos de seguridad**. Hasta que las organizaciones comiencen a implementar medidas de seguridad centradas en la identidad, los ataques que vulneran la seguridad de las cuentas de los usuarios continuarán proporcionando un camuflaje perfecto para las violaciones de datos. Por lo tanto, el camino hacia la Confianza Cero siempre debe comenzar con la identidad.

La Confianza Cero es solo para grandes organizaciones:

Google fue una de las primeras compañías en adoptar el modelo de Confianza Cero. Como resultado, muchas personas todavía piensan que es solo para las grandes empresas. Pero la realidad es que nadie está a salvo de un ciberataque. De hecho, **el 61% de todas las violaciones de datos afectaron a las pequeñas empresas en 2018**. El tamaño o el presupuesto de la empresa no deberían ser un elemento disuasorio porque incluso las empresas más pequeñas pueden comenzar con el Zero Trust adoptando un enfoque simplificado. Por ejemplo, muchas organizaciones pueden fortalecer significativamente su seguridad creando una barrera basada en contraseñas o en sistemas de autenticación.

Necesidad de extraer y reemplazar toda la red de entorno de seguridad:

Es cierto que cuando Google estableció por primera vez su arquitectura de seguridad de Confianza Cero, decidió reconstruir toda su red de seguridad desde la base. Pero este no es el caso de la mayoría de las organizaciones. La Confianza Cero puede implicar simplemente un aumento de los controles de seguridad que ya existen en el entorno. Por ejemplo, **se puede comenzar implementando una solución "MFA en todas las áreas"**. Este primer paso puede ser de gran ayuda para establecer un seguro de identidad y reducir drásticamente la superficie de ataque.



La Confianza Cero se limita a la implementación en el sitio:

Muchas organizaciones piensan que la Confianza Cero solo puede funcionar en las instalaciones físicas y no se puede aplicar a la nube pública. Esto se convierte en una preocupación cuando los datos confidenciales residen fuera del perímetro de la red tradicional. La Confianza Cero puede extenderse fácilmente a los entornos de la nube, y es cada vez más importante hacerlo a medida que las organizaciones de una amplia gama de industrias se trasladan a entornos híbridos y multi-Cloud. Además, la Confianza Cero **no solo cubre la infraestructura, las bases de datos y los dispositivos de red, sino que se extiende a otras superficies** de ataque que se están convirtiendo cada vez más en requisitos estratégicos de las organizaciones modernas.

El único beneficio del Zero Trust es minimizar la exposición al riesgo:

La mitigación del riesgo es claramente un beneficio importante de Zero Trust, pero definitivamente no es el único. Los últimos informes concluyen que **la Confianza Cero puede reducir la exposición al riesgo de una organización en un 37% o más**. Sin embargo, también descubrieron que las organizaciones que implementan esta política pueden reducir los costes de seguridad en un 31% y ahorrar millones de dólares en sus presupuestos de TI. La Confianza Cero también puede conducir a una mayor confianza empresarial. Las organizaciones que implementan Zero Trust tienen un 66% más de confianza en la adopción de modelos de trabajo móvil y un 44% más de confianza en la seguridad de los entornos DevOps. Como resultado, pueden acelerar nuevos modelos de negocio e introducir nuevas experiencias de clientes con un mayor sentido de seguridad y éxito.



RETOS DE SEGURIDAD BLOCKCHAIN:

El Blockchain se enfrenta a una tercera ola. La primera estuvo protagonizada por el Bitcoin, y servía casi exclusivamente para la transferencia de dinero. Tras ella llegó la plataforma de Smart Contracts Ethereum, como ejemplo más representativo de la conocida como segunda ola, que permitía ejecutar una lógica más compleja más allá de las transferencias de dinero.

Los retos de la tercera ola del Blockchain pasan por:



La escalabilidad. Capacidad de aumentar las transacciones por segundo, manteniendo la seguridad. El Blockchain tiene cuatro retos relacionados con la escalabilidad: las limitaciones, el tamaño de bloque, el tiempo de respuesta y las altas tarifas. Todos estos problemas deben resolverse con premura ya que la red crece a pasos agigantados.



La privacidad. La necesidad de establecer canales privados entre los actores que usen esta tecnología. Esto es un gran problema para las empresas que manejan datos sensibles y necesitan tener los límites muy definidos, ya que sus clientes confían en ellos. Pero, si los datos están almacenados en un enorme sistema público, ¿cómo lograr privacidad? Parece que la única solución es cambiar los registros para limitar el acceso a los datos, un reto que aún está por definir.



Procesar tiempo y potencia. El consumo de energía es otro desafío ya que, en su mayor parte, se sigue usando la infraestructura de la moneda virtual Bitcoin, utilizando Proof of Work como un algoritmo de consenso. Para mantener el sistema en funcionamiento, la minería necesitará mucha potencia de cálculo. Si se traduce al procesamiento diario de grandes volúmenes de datos, esta gestión alcanza un coste muy elevado.



La sostenibilidad. Es decir, la necesidad de pasar del actual modelo de financiación basado en las ICOs (mediante el cual se generan 'tokens' para proporcionar flujo inicial de dinero), hacia un modelo en el que las empresas reciban un flujo constante de dinero en el tiempo para poder ser más sostenibles. Además, este punto también está relacionado con la cantidad de electricidad que se necesita para la minería, lo que hace a este sistema muy poco amigable con el medio ambiente, necesitando urgentemente una nueva fuente de alimentación más sostenible.



La regulación legal. Las acciones para crear y actualizar las reglas implícitas o explícitas de un sistema 'Blockchain'. Estas reglas pueden ser código, leyes, procesos o responsabilidades. Además, aunque muchas organizaciones ya están usando el Blockchain como un medio de transacción, no hay una regulación específica al respecto.



Almacenamiento. El Blockchain elimina la necesidad de un servidor central para almacenar las transacciones e identificaciones de los dispositivos, pero los datos deben almacenarse en los mismos nodos, lo que provoca que aumente de tamaño a medida que pasa el tiempo. Al final, sobrepasará la capacidad de almacenamiento de los dispositivos inteligentes que existen hoy en día.



Interoperabilidad. Capacidad de las diferentes plataformas Blockchain para comunicarse entre sí y con las infraestructuras del sistema financiero tradicional.





Tipología de ataques de seguridad.

03

Conforme crece la importancia de las nuevas tecnologías en la economía global, mayor es el valor que empresas y usuarios atribuyen a sus infraestructuras informáticas y activos digitales. El potencial impacto de un ciberataque es hoy cientos de veces mayor que hace cuarenta años, teniendo en cuenta los posibles daños materiales (paralización de la producción) e inmateriales (robo de datos de negocio, violación de la privacidad de los usuarios).



CRYPTOJACKING:

El Cryptojacking o minado de Criptomonedas deriva de la conjunción de Cryptocurrency (Criptomonedas) y Hijacking (Secuestro), y se define como el **uso no detectado de un dispositivo informático ajeno para extraer monedas digitales**. Es la vulneración de un ordenador, Smartphone o red de equipos, no para acceder a datos, sino para minar criptomonedas secuestrando recursos de otros.

Minar en busca de criptomonedas es una tarea compleja y que consume muchos recursos, tanto energéticos como computacionales. En ese contexto los ciberdelincuentes han descubierto una forma de hacerlo más fácil: **entrando en ordenadores ajenos y haciendo que sean esos los equipos que realicen los cálculos necesarios**, consumiendo sus propios recursos, para obtener divisas digitales.

El auge del Cryptojacking ha ido aparejado al alza de las cotizaciones de las monedas virtuales, además de que se caracteriza por ser fácil de efectuar y automatizar, con la dificultad de detectar su presencia en el dispositivo infectado. Durante el año 2017 se produjo **un incremento del 34.000% en ataques** relacionados con el Cryptojacking. Tan sólo en los tres últimos meses de 2017 el crecimiento fue del 8.500 %.

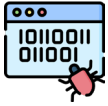
¿CÓMO SE INFECTA UN EQUIPO?

Hay varias formas posibles de secuestrar la capacidad computacional de un dispositivo. El modo más frecuente es la infiltración de Malware: en cualquier momento (al recibir un correo, instalar una aplicación, activar un software oculto, etc.) el ciberdelincuente puede instalar en el equipo objetivo un Malware que consiga disparar el uso de la CPU y empezar a minar criptomonedas sin conocimiento del usuario. Una vez infectado el equipo, el Cryptojacker comienza a trabajar a todas horas para extraer criptomonedas, manteniéndose oculto en segundo plano.

Pero existen también otros modos de infección, como la **integración de mineros en el navegador**. Es una práctica cada vez más frecuente: algunas webs, sin avisar a sus usuarios, ofrecen la conexión a Internet para el minado, lo que supone un fraude para las personas que estarán poniendo su equipo al servicio de un tercero. A través del navegador utilizan el ancho de banda y equipo del usuario para generar nuevas criptodivisas.



OBJETIVO DE LOS ATAQUES



Código dañino. El objetivo es reducir la complejidad del proceso de minado al repartir el esfuerzo computacional entre el mayor número de ordenadores posibles, y por tanto reducir el tiempo de obtención de las criptomonedas. Un ejemplo es Njw0rm, un Malware perteneciente a la familia RAT (Remote Administration Tool) muy propagado por Oriente Medio y que evolucionó para añadir minado de Bitcoin.



Correos fraudulentos. Mediante campañas de Spam el atacante puede tratar de engañar al usuario para que descargue y ejecute un programa que supuestamente es legítimo, pero que en realidad es un Cryptominer.



Exploit Kits. Son herramientas que automatizan la búsqueda de vulnerabilidades en un sistema para poder infectarlo. Normalmente se aprovechan de errores en el navegador o de algún complemento instalado para realizar la descarga del código dañino.



IoT. Cada vez más dispositivos electrónicos de uso cotidiano disponen de acceso a internet, lo que supone una gigantesca red de equipos interconectados que podrían usarse de manera malintencionada, como por ejemplo para minar criptomonedas.



Web-based. Aquellas formas de minado que se aprovechan de los visitantes de una página web en la que se ejecuta, en la mayoría de los casos, un código en JavaScript que realiza el minado de forma discreta.



Dispositivos móviles. Los dispositivos móviles también se han visto afectados por este nuevo tipo de amenaza. Los Cryptominers se suelen encontrar en Apps piratas que ofrecen falso contenido premium gratis.



Servidores. Los cibercriminales buscan infectar, en muchos casos, grandes servidores gracias a su alta capacidad de cómputo y así aumentar su capacidad de minado. Usan técnicas específicas para atacar servidores, como la explotación de vulnerabilidades, fuerza bruta, inyección SQL, etc.

RIESGOS ASOCIADOS

El mayor peligro del Cryptojacking no es sólo el acceso a los ordenadores personales domésticos, sino que acabe inundando los equipos de toda una empresa, provocando diversos perjuicios: por una parte, la empresa acabará experimentando un tremendo aumento de la factura eléctrica, ya que el Cryptojacking exprimirá cada equipo y recurrirá a él siempre que pueda.

Por otra parte, los ordenadores normales no están preparados para funcionar mientras minan criptomonedas. Si el Cryptojacking infecta el dispositivo, **creará problemas a la empresa por la pérdida productividad y por los gastos adicionales**, ya que se requiere asistencia técnica o, en ocasiones, la sustitución del ordenador.

IA COMO PUNTO DE ATAQUE: DEEP FAKE:

La IA también amplía el alcance de las Ciberamenazas, dado que **mejora de forma clara la eficiencia, escalabilidad, multiplicidad y efectividad de los ciberataques**, además de favorecer el anonimato y el distanciamiento psicológico del atacante.

Automatización de ataques de Phishing personalizados basados en ingeniería social.

La información online de las víctimas se utiliza para generar automáticamente documentos (ej: sitios web, correos electrónicos o enlaces maliciosos) personalizados en los que probablemente harán clic, enviados desde direcciones que se hacen pasar por sus contactos reales, utilizando un estilo de escritura que imita a esos mismos contactos. Esta amenaza crecerá a medida que la IA se desarrolle más, gracias a Chatbots capaces de generar más confianza al poder mantener diálogos más largos, y a los DeepFakes de video y audio.

Ataques de denegación de servicio que imitan la navegación de personas reales.

Imitando el comportamiento humano (por ejemplo, a través de patrones de clic de velocidad humana y navegación en el sitio web), un ejército de Bots puede saturar un servicio en línea e impedir el acceso de usuarios legítimos.

Automatización de tareas en el cibercrimen: por ejemplo, el diálogo y el procesamiento de transacciones a víctimas de Ransomware.

La selección y priorización de objetivos a partir de su comportamiento en la red.

Debido al acceso a grandes conjuntos de datos, es posible identificar a las víctimas de manera más eficiente, por ejemplo, mediante la estimación de la riqueza personal y la disposición a pagar en función del comportamiento en línea.

La alteración de algoritmos de IA.

Las GAN (Redes Generativas Antagónicas) enfrentan a dos redes neuronales entre sí, y permiten adivinar cuáles son los algoritmos utilizados por los sistemas de seguridad en sus modelos de IA. Además, los atacantes pueden identificar los conjuntos de datos utilizados para entrenar los modelos para contaminarlos; por ejemplo, cambiando las etiquetas de las muestras de código malicioso para indicar que son seguras y no sospechosas.

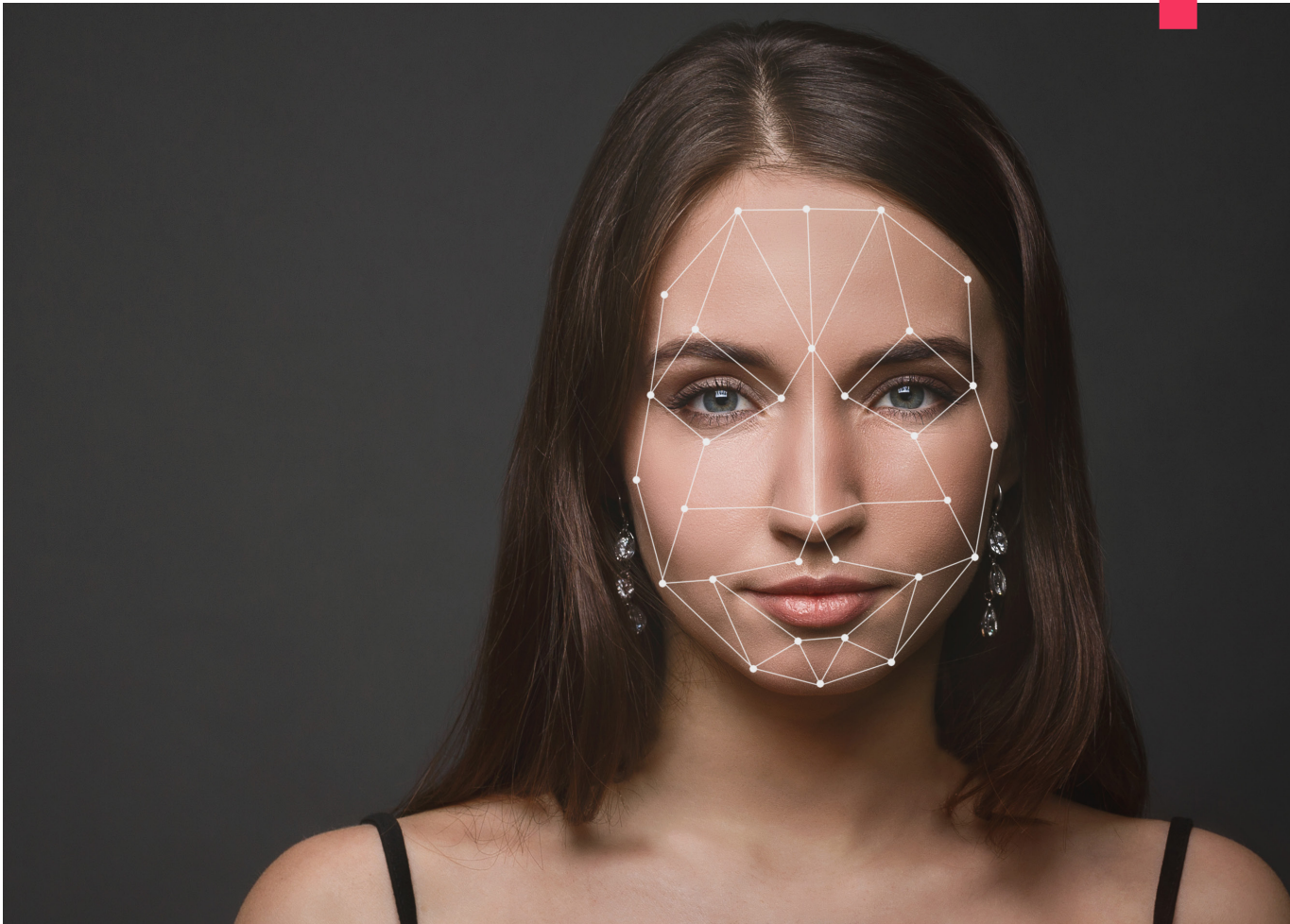


VÍDEOS Y AUDIOS FALSOS

El desarrollo de la IA está permitiendo crear mensajes de audio y vídeo falsos difícilmente distinguibles de los reales. Son conocidos como DeepFakes, y para hacerlo, se utilizan las Redes Generativas Antagónicas (RGAs), una clase de algoritmo que permite crear nuevos tipos de datos a partir de otros conjuntos que ya existen. Por ejemplo, una RGA puede analizar grabaciones de voz de una persona, para posteriormente crear un audio totalmente nuevo que tenga el mismo tono y timbre y que utilice el mismo lenguaje.

Estos DeepFakes están siendo una puerta de entrada para los ciberdelincuentes. Ahora, los correos electrónicos de Phishing creados mediante IA que tienen como objetivo engañar a las personas para que entreguen sus contraseñas y otros datos confidenciales, han alcanzado un nuevo nivel. **Los atacantes pueden contar con estos videos y audios para reforzar las técnicas de Phishing.**

Además de las implicaciones en el mundo cibernético, los DeepFakes pueden ser utilizados en el mundo físico, por ejemplo, para **volatilizar el precio de las acciones de una empresa después de publicarse un mensaje falso de su CEO** con informaciones negativas sobre la compañía. Otro ejemplo es el de los videos que se usan para difundir noticias falsas en cuestiones políticas, para influir en elecciones o cuestiones geopolíticas.



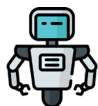
MACHINE LEARNING PARA ATAQUES AUTOMATIZADOS:

Los analistas de Ciberseguridad coinciden en pronosticar un **auge de los ataques cibernéticos automatizados en los próximos años**, los cuales se multiplicarán y propagarán gracias a, entre otros factores, la expansión del IoT, aumentando masivamente el potencial daño a provocar. Algunos de los ataques automatizados que más han evolucionado, y que ya están experimentando un importante auge son:



Adivinación de contraseña:

Sistemas informáticos capaces de probar múltiples combinaciones de credenciales de forma automática, para hacerse con contraseñas y entrar a cuentas en línea de forma ilícita. Debido a que muchas personas reutilizan sus contraseñas para acceder a las diferentes plataformas online, los ciberdelincuentes han encontrado aquí un filón para innovar buscando métodos que pueden causar un enorme daño potencial. El aprendizaje automático se usa para registrar combinaciones de números y letras más habituales y probar millones de ellas en un tiempo récord.



Hacker Bots:

Funcionan suplantando la personalidad de un supuesto usuario real para, una vez burlado el sistema, poder acceder al mismo para robar la información en cuestión de segundos, antes de que puedan ser detectados por la organización víctima del ataque.



Extorsión mediante Bots:

Este tipo de ataque tiene como objetivo dañar la reputación de una empresa mediante la publicación masiva de valoraciones negativas en la web y/o reseñas de quejas hacia una compañía; o bien entrando dentro del sistema y amenazando con llevar a cabo publicaciones negativas en nombre de la organización atacada a menos que se pague para evitarlo.



Fuzzing:

Esta técnica se sirve de herramientas que introducen posibles combinaciones mediante permutaciones de datos (como un campo de texto, un archivo o la combinación de botones, etc.) con el fin de detectar cuál destapa un agujero de seguridad. Este sistema, de gran complejidad, está empezando a ser aprovechado también por los ciberdelincuentes gracias a la posibilidad de automatizarlo mediante modelos de Machine Learning. Al emplear estos algoritmos es posible reducir el número de combinaciones que se efectúan sobre el programa, ya que la herramienta va aprendiendo del estado del software con cada iteración, calculando patrones más propensos a causar una inestabilidad y descartando aquellos que no causarían ningún efecto.

MACHINE LEARNING COMO RESPUESTA

La mejor forma de responder a un ataque automatizado es emplear igualmente mecanismos de defensa automatizados. Es decir, **utilizar el aprendizaje automático para predecir situaciones de riesgo, identificar patrones de uso anómalos** y, en definitiva, protegerse frente a los ataques basados en IA. Y es que la cantidad de datos y la velocidad de procesamiento que pueden alcanzar los ataques automatizados son imposibles de abarcar desde una monitorización manual.

El Machine Learning se viene empleando desde hace algún tiempo para la ciberdefensa, mediante la implantación de herramientas automáticas capaces de recopilar enormes volúmenes de datos, para así **identificar con el máximo detalle el comportamiento habitual de los procesos** y detectar después cuando podrían estarse produciendo anomalías.

Estas herramientas de Inteligencia Artificial y Machine Learning beben de **múltiples fuentes de datos procedentes de centros de seguridad** (internos y externos a la organización), sistemas informáticos de los diferentes departamentos, rastreo en Internet, etc., que después cruzan para predecir los posibles movimientos de los ciberdelincuentes.



FRAUDE DEL CEO:

En los últimos años se han dado muchos casos de la llamada "estafa o fraude del CEO": un empleado recibe un correo urgente del CEO pidiéndole que haga una transferencia a una cuenta bancaria en el extranjero, cuando en realidad ese correo lo ha enviado un impostor. Según el **FBI este fraude ya ha costado más de 2.000 millones de dólares a nivel mundial.**

Este ciberdelito es una de las variantes más recientes y específica de los ataques de Phishing basados en correo electrónico. En resumen, este fraude suele ejecutarse, principalmente, a través del correo electrónico por una de estas dos vías:

Suplantando la identidad de un proveedor habitual: en el correo electrónico, por ejemplo, se solicita al empleado la modificación de un número de cuenta en el que realizar un pago.

Suplantando la identidad de un alto directivo o socio de la empresa: se solicita a la víctima que lleve a cabo una operación corporativa confidencial o urgente, como la adquisición de una compañía en el extranjero o un bien inmueble.

Una vez que el dinero sale de las cuentas, **seguirle el rastro es casi imposible, ya que son redes internacionales que operan desde distintos puntos** del planeta, con múltiples servidores con los que simulan 'e-mails' de la empresa o de firmas de servicios profesionales.

Existen diversas campañas que están actualmente activas y con diferentes niveles de sofisticación. Los más básicos emplean el 'Spear Phishing E-mail' con errores semánticos y direcciones de correo falsas, pero fácilmente reconocibles. Sin embargo, existen campañas más

complejas combinando ingeniería social (por teléfono y e-mail) donde el cibercriminal tiene información sobre su víctima obtenida de la web o incluso a través de Malware.

Los intentos cada vez son más refinados. Combinan llamadas y correos electrónicos que imitan a algún ejecutivo de alto nivel, con comunicaciones breves, concisas y muy ejecutivas. También se apoyan en envíos ficticios desde consultoras o bufetes proveedores de la empresa atacada, y se usa alguna operación en la que esté inmersa, ya sea una adquisición o importación de productos (cualquier operativa que pueda justificar un pago). **La persona elegida siempre tiene capacidad para hacer transferencias en nombre de la compañía.**



VAP: VERY ATTACKED PERSON

Los cibercriminales no solo intentan suplantar a los cargos VIP de las empresas (CEO, directores generales o presidentes del consejo de administración) cuando plantean sus ataques, sino que empiezan a **apuntar a perfiles de menor nivel jerárquico, en concreto a los VAP** (Very Attacked Person).

Se trata de profesionales que están uno o varios peldaños por debajo en la jerarquía, pero que, **por su puesto y responsabilidad, cuentan con ciertos accesos y privilegios**. Estos VAP no son necesariamente personas conocidas o monitorizadas de forma activa por los equipos de seguridad, por lo que los cibercriminales pueden tener mayor éxito en sus propósitos sin llamar la atención.

No hay un perfil definitivo de VAP y varía según la empresa y el sector.

Sería, por ejemplo, el asistente del CEO, un programador que maneja los códigos de acceso en remoto o alguien del equipo financiero que se encarga de hacer los pagos a proveedores.

Como también pasaba en la estafa del CEO, el ataque más habitual a un VAP tiene como destino el correo electrónico y suele traducirse en una suplantación de identidad. Una vez el delincuente es capaz de hacerse pasar por el empleado con privilegios, podrá hacer casi cualquier cosa: desde **solicitar transferencias fraudulentas y obtener credenciales a robar datos confidenciales** de la empresa. Con frecuencia, estos estafadores envían a otros empleados emails falsos categorizados como urgentes para acelerar el robo.



AMENAZAS FILELESS:

El Fileless Malware está creciendo a pasos agigantados durante los últimos años, siendo una de las principales amenazas de seguridad para la próxima década.

El Fileless Malware es una amenaza para el ordenador que carece de soporte en un fichero, amparándose y **ejecutándose a través de la memoria RAM del dispositivo**. El principal problema, y a diferencia de otros Malware, es que no hay prácticamente soluciones de antivirus que sean capaces de limpiar este tipo de amenazas. Al tratarse de un ataque que se esconde y ejecuta a través de la memoria RAM del dispositivo, si se apaga el ordenador, en teoría se eliminará. Esto es válido para un ordenador de usuario, pero no para un sistema de empresa que se mantiene encendido las 24 horas del día.

Este tipo de Malware sin archivos tiene una gran tasa de éxito en sistemas de empresas, también debido a la **falta de herramientas de software antimalware para detectar este tipo de amenaza**. Y es que tal como ha pasado con el Ransomware, los ciberdelincuentes perciben que es más rentable atacar a las empresas que a los propios usuarios.

La evolución hacia ataques Fileless era un paso natural dada la inmensa flexibilidad ofrecida por intérpretes como Powershell. Este tipo de ataques han representado un 35% del total de ataques registrados en ordenadores durante 2018, y se estima que para finales de este año se podría alcanzar el 50% de los ataques totales de Malware.



CLASIFICACIÓN DE AMENAZAS

Dado que los ataques implican varias fases de funcionamiento, como la ejecución, la persistencia o el robo de información, algunas partes de la cadena de ataque pueden no relacionarse con archivos, mientras que otras pueden implicar el sistema de archivos de algún modo.

Las amenazas sin archivos se **pueden clasificar según su punto de entrada**, lo que indica la forma en que el Malware sin archivos puede llegar a un equipo. Pueden llegar a través de un ataque por medio de hardware comprometido, o a través de la ejecución regular de aplicaciones y scripts. Por ejemplo, las vulnerabilidades se pueden basar en archivos o datos de red, los Peripheral Component Interconnect (PCI), un tipo de vector de hardware, siendo los scripts y los ejecutables subcategorías del vector de ejecución.

También es posible clasificar el anfitrión de la infección. Por ejemplo, una aplicación Flash que puede contener una vulnerabilidad, un ejecutable simple, un Firmware malintencionado desde un dispositivo de hardware o un MBR infectado, que podría iniciar la ejecución de un Malware antes de que el sistema operativo se cargue. Evidentemente, las categorías no son iguales: algunas son más peligrosas, pero también más difíciles de implementar, mientras que otras se usan más frecuentemente a pesar de que no son muy avanzadas.

Desde esta categorización se pueden recopilar tres tipos principales de amenazas sin archivos en función de la cantidad de huella que pueden dejar en los aparatos infectados:

Tipo I (no se realizó actividad de archivo):

Un Malware sin archivos se puede considerar uno que nunca necesita escribir un archivo en el disco. Las infecciones de este tipo pueden ser más difíciles de detectar y remediar. Por lo general, los productos antivirus no tienen la capacidad de acceder al Firmware para la inspección; incluso si lo hicieran, sería extremadamente complicado detectar y remediar las amenazas en este nivel. Debido a que este tipo de Malware

sin archivos requiere altos niveles de sofisticación y a menudo depende de una configuración de hardware o software determinada, no es un vector de ataque que se pueda explotar de forma fácil y confiable. Por esta razón, aunque sea extremadamente peligrosa, las amenazas de este tipo tienden a ser poco frecuentes.

Tipo II (actividad de archivo indirecta):

Hay otras maneras en las que el Malware puede lograr presencia sin archivos en un equipo sin necesidad de un esfuerzo significativo de ingeniería. Este tipo de Fileless no escribe directamente archivos en el sistema de archivos, pero los puede usar indirectamente. Es posible realizar dicha instalación mediante la línea de comandos sin requerir la presencia de la puerta trasera, por ejemplo. Por lo tanto, el Malware puede instalarse y ejecutarse sin tocar el sistema de archivos.

Tipo III (archivos necesarios):

Ciertos programas malintencionados pueden contener algún tipo de persistencia sin archivos, pero no usar archivos para funcionar. Un ejemplo de este tipo sería Kovter.



HOST DE INFECCIONES

Esta clasificación cubre la panorámica de lo que se suele denominar Fileless:

Explote:

- **Basado en archivos:** ejecutable, Flash, Java, documentos, etc.
- **Basado en red:** una comunicación de red que se aprovecha de una vulnerabilidad en el equipo de destino puede lograr la ejecución de código en el contexto de una aplicación o del núcleo. Ejemplo: WannaCry

Hardware:

- **Basado en dispositivos:** tarjeta de red, disco duro, etc.
- **Basado en CPU:** las CPU modernas son extremadamente complejas y pueden incluir subsistemas que ejecuten Firmware con fines de administración. Dicho Firmware puede ser vulnerable a secuestros y permitir la ejecución de códigos maliciosos que, por lo tanto, funcionarían desde dentro de la CPU.

- **Basado en USB:** los dispositivos USB de todos los tipos se pueden reprogramar con Firmware malintencionado capaz de interactuar con el sistema operativo de varias maneras. Este es el caso de la técnica de BadUSB.
- **Basado en BIOS:** es un Firmware que se ejecuta dentro de un conjunto de chips. Se ejecuta cuando un equipo está encendido, inicializa el hardware y, después, transfiere el control al sector de inicio. Es un componente muy importante que funciona a un nivel muy bajo y se ejecuta antes del sector de inicio. Es posible reprogramar el firmware de BIOS con código malicioso.
- **Basado en Hypervisor:** las CPU modernas proporcionan compatibilidad con el Hypervisor de hardware, lo que permite al sistema operativo crear máquinas virtuales sólidas. Una máquina virtual se ejecuta en un entorno simulado y, en teoría, no es consciente de la emulación. Un Malware que toma el control de un equipo puede implementar un pequeño Hypervisor para ocultarse a sí mismo fuera del territorio del sistema operativo en ejecución.

Ejecución e inyección:

- **Basado en archivos:** ejecutables, DLL, archivos LNK, tareas programadas, etc.
- **Basado en macros:** el lenguaje VBA es una herramienta flexible y eficaz diseñada para automatizar la edición de tareas y agregar funcionalidad dinámica a los documentos. Pueden ser abusados por intrusos para lanzar operaciones malintencionadas, como descodificar, ejecutar o inyectar una carga útil, o incluso implementar un Ransomware completo. Por ejemplo, documentos de Office.
- **Basado en secuencias de comandos:** archivo, servicio, registro, repositorio WMI, Shell, etc.
- **Basado en disco:** registro de inicio. Ejemplo: Petya.



PHISHING, FARMING, FAKE NEWS:

En los últimos años, los cibercriminales han pasado de atacar la infraestructura informática de una compañía, a poner su **punto de mira en las personas** que forman parte de la misma. Mientras que la seguridad de los distintos componentes informáticos que se integran en una compañía ha mejorado exponencialmente, el ser humano sigue incurriendo en errores.

Mientras que la mayoría de los ataques dirigidos contra las empresas entran en alguna categoría de Phishing, Spoofing o de suplantación de identidad, las grandes empresas **destinan menos del 10% de su presupuesto de seguridad informática en proteger el área más crítica y susceptible de ataque:** la identidad online de sus empleados (correo corporativo y personal, cuentas en la nube, etc.).

TIPOS DE ATAQUES

Los ataques de Phishing son una de las infracciones de Ciberseguridad más conocidas, **engañando a las personas para que compartan información confidencial** como contraseñas y números de tarjetas de crédito. Pero a pesar de sus muchas variedades, el denominador común es el uso de un pretexto fraudulento para adquirir datos valiosos. Algunas categorías principales:

Phishing tradicional o Deceptive Phishing.

Modalidad más común de Phishing. El hacker se hace pasar por alguien conocido o por una marca que cuente con la confianza de la víctima. Por lo general, el usuario recibe un correo electrónico en el que se incluye un enlace que apunta a un sitio malicioso. Puede ser una página clonada cuya URL es prácticamente igual a la del sitio legítimo. Otra opción es que el hacker haya introducido algún tipo de iframe en una página legítima, aprovechando alguna vulnerabilidad de ésta.

Malware-Based Phishing. Este tipo de ataque se caracteriza por el envío de correos electrónicos en los que se introduce una pieza de Malware como archivo adjunto o como un descargable en el sitio web al que apunta el hipervínculo enviado por email y así poder aprovechar las vulnerabilidades del dispositivo del usuario. Este tipo de ataque es especialmente común en las pequeñas y medianas empresas, ya que por lo general, el software no está siempre actualizado a la última versión y presenta mayores vulnerabilidades.





Spear Phishing. En esta modalidad, el ataque suele ser mucho más personalizado. En algunos casos se llega incluso a incluir el nombre de la víctima, su posición, la compañía, el teléfono, etc. Además, suelen ir dirigidos a un número reducido de personas con cierto perfil dentro de una empresa (normalmente suele ser el eslabón más débil). El objetivo de este tipo de ataques suele ser más específico. Lo más común es que el vector de ataque utilizado sea el email o las redes sociales.

Smishing (SMS). Este tipo de Phishing no es realizado por email, sino a través de los teléfonos móviles. El hacker suele hacerse pasar por una empresa de confianza y envía un SMS informando al usuario de que ha ganado un premio, ofreciéndole participar en un sorteo o para ofrecerle algún tipo de atención/soporte. Para canjearlo, la víctima debe hacer clic en un hipervínculo, llamar a un n° de teléfono o responder al mensaje.

Vishing. El término viene de "Phishing de voz" e implica el uso del teléfono. En este tipo de ataque, o bien el ciberdelincuente establece centros de atención telefónica o directamente lanza él las llamadas. Se hace pasar por algún proveedor, operador, un centro de soporte, un banco, etc. con el objetivo de recabar cierta información personal.

Pharming. Los cibercriminales manipulan los archivos hosts de una empresa o el sistema de nombres de dominio de esta. Como resultado, las solicitudes de URL devuelven una dirección falsa y las comunicaciones se dirigen a un sitio web falso. Los usuarios introducen sus credenciales o información confidencial en el mismo, sin saber que está controlado por los cibercriminales.

Búsquedas del navegador o SEO Phishing. Consiste en posicionar una página falsa por encima de la oficial mediante técnicas de SEO y SEM, para que cuando la víctima realiza una búsqueda, acceda a dicho resultado por error y, creyendo que se trata de la página legítima, introduzca en ella algún tipo de información.

Phishing de clonación. En este ataque, los delincuentes hacen una copia, o clonan, correos electrónicos legítimos enviados anteriormente que contienen un enlace o un archivo adjunto. Luego, el autor del Phishing sustituye los enlaces o archivos adjuntos con contenido malicioso disfrazado para hacerse pasar por el auténtico.

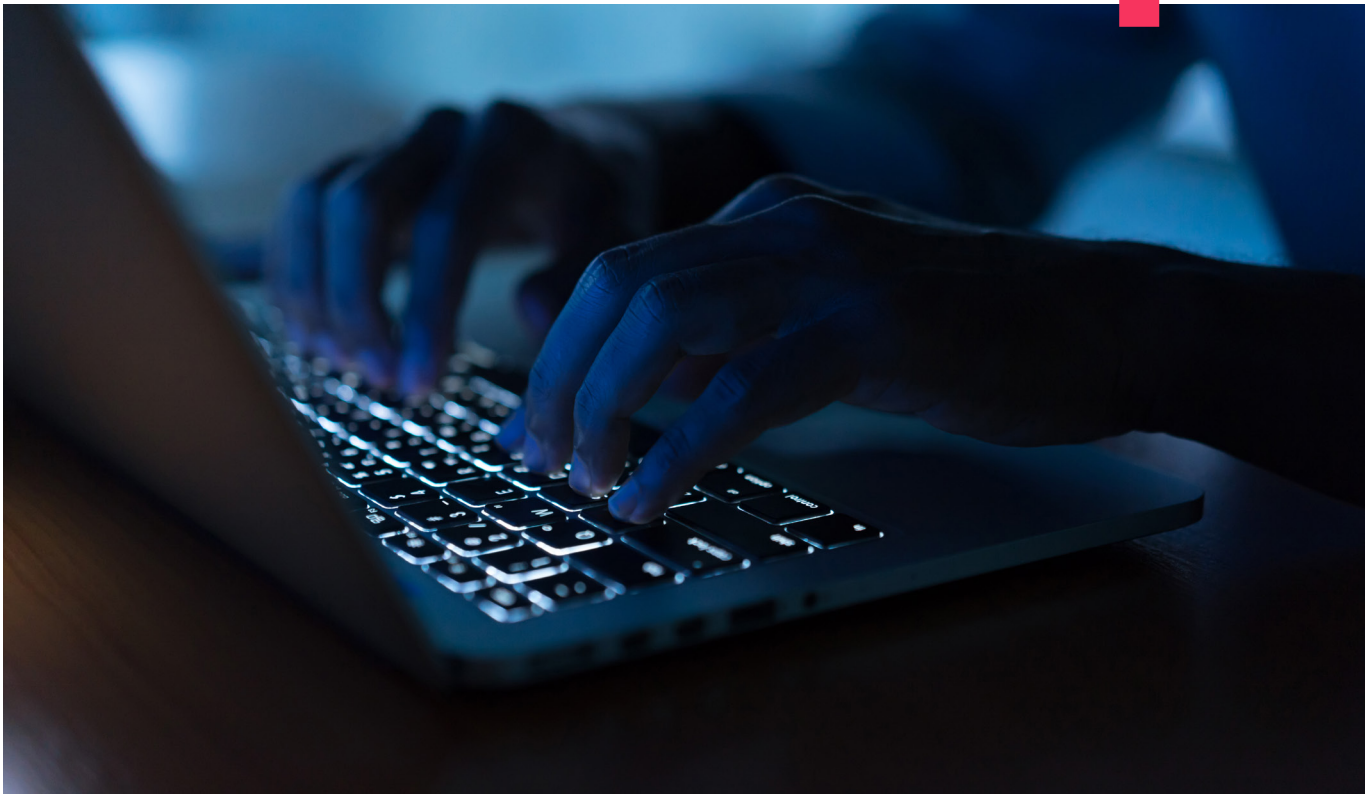
FAKE NEWS

Las noticias falsas están cada vez más estandarizadas en la sociedad y pueden repercutir en la reputación de las empresas. A pesar de que el término 'Fake News' comenzó a usarse desde hace relativamente poco tiempo, las noticias falsas han estado presentes desde la aparición de la prensa. Lo realmente novedoso ha sido el fenómeno que hay detrás, así como el **negocio edificado sobre la mentira y su difusión masiva**.

Hay que referirse a 'Fake News' como información falsa propagada bajo la voluntad intencionada de desinformar al interlocutor. Se publican en portales de noticias, prensa escrita, radio, televisión y redes sociales, llegando al público de manera masiva. Cuentan con dos características principales: en primer lugar, adquieren una apariencia de noticia real y en segundo, **tienen un objetivo definido, normalmente económico o ideológico**.

Estas noticias están marcadas por la 'dictadura del clic', es decir, **necesitan tráfico constante para generar ingresos económicos**. Esta es la razón por la que cuanto más viral es el contenido, el responsable recibe más dinero y por lo tanto, más 'Fake News' son difundidas. Es posible automatizar la creación de bulos, siendo más barata su producción y más fácil su difusión a través de las RR.SS.

Ejemplos concretos podrían ser: enviar una serie de emails maliciosos que incluyan información falsa y vídeos sobre una empresa, o una noticia falsa que llame la atención del lector, para incluir en realidad algún tipo de Malware. De manera similar, Fake News compartidas masivamente en Facebook y Twitter podrían ser en realidad estrategias para atacar a los usuarios mediante Phishing, convirtiendo el Clickbaiting en Clickjacking.



RANSOMWARE:



El Ransomware, también conocido como “secuestro de datos” es un tipo de ataque que se sirve de un programa dañino capaz de **impedir el acceso a determinadas partes o archivos del sistema operativo** infectado, con la finalidad de exigir después un rescate a cambio de liberar el sistema eliminando la restricción.

El gran riesgo de este ataque radica en el grave daño que puede provocar a la imagen corporativa de las empresas, además de las **pérdidas económicas que se derivan de la paralización de su actividad**. Es por este motivo que las empresas suelen ser propensas a pagar por el rescate de los datos antes que tener que hacer frente a estos otros inconvenientes.

Los ataques de Ransomware se hicieron muy populares especialmente en el 2017 a raíz del secuestro masivo de datos que sufrieron importantes empresas de todo el mundo como consecuencia de la expansión del virus Wannacry. A día de hoy, la estadísticas muestran cómo desde ese año el nº de ataques se ha reducido y la incidencia se produce a una escala mucho menor, siendo las **principales víctimas pequeñas empresas y autónomos** donde existen menores medidas de seguridad.

En los últimos años los ciberdelincuentes han ido abandonado las técnicas de infección masiva de grandes empresas para centrarse en ataques de menor escala, enfocados a empresas que a priori podrían ser más propensas a pagar rescates para evitar la pérdida de su actividad. También **se están viendo más afectadas aquellas empresas que operan en sectores industriales estratégicos**, debido a las graves implicaciones económicas y de reputación que conlleva un bloqueo.

Las dificultades para luchar contra el Ransomware radican en su complejidad como Malware, pues **para secuestrar los archivos utiliza una herramienta legítima como es el cifrado de datos**, que otros muchos programas normales usan a diario al desarrollar sus funciones.

INFRAESTRUCTURAS CRÍTICAS Y OPERADORES DE TECNOLOGÍA:

Tras la aprobación de la **nueva Directiva NIS** (normativa de la Unión Europea que busca mejorar la seguridad de las redes y sistemas de información en su territorio), que obliga a todos los operadores de infraestructuras críticas y a los operadores esenciales (OT) a proteger de forma adecuada sus redes y sistemas de información, además de obligarles a notificar incidentes, este área resulta prioritario en la agenda de Ciberseguridad global.

Las infraestructuras críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un **impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos** o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas.

Son todas aquellas **infraestructuras cuyos sistemas, medios y servicios son fundamentales para el sostenimiento social** y que aseguran la continuidad en el funcionamiento normal de los servicios prestados por los Estados y Administraciones Públicas.

La preocupación por la Ciberseguridad radica en dar continuidad a la actividad y los servicios prestados a los ciudadanos. **Una mínima interrupción del servicio puede generar un alto impacto sobre una organización** y, por consiguiente, un gran número de personas.

Dada la importancia que tienen las infraestructuras críticas y el contexto geopolítico actual, el empleo de ciberataques como elemento destabilizador se ha convertido en una realidad. A su vez, el objetivo de los ciberataques ha cambiado. El beneficio económico buscado por los ciberdelincuentes pasa a un segundo plano, pues se buscan vulnerabilidades en los sistemas de las infraestructuras críticas con fin de **obtener información relevante, tomar el control de una actividad o de una organización completa y/o** paralizar su actividad.

Las consecuencias pueden ser nefastas: desde un país entero sin luz, sistemas de tratamiento de agua deficientes, filtrado de datos sanitarios, caída de redes de telecomunicaciones, fallos en sistemas de transporte, etc.





SHADOW IT:

La irrupción de los servicios Cloud supone un incremento de la productividad gracias a una mayor agilidad de los procesos y una mejor disponibilidad de la información. Cada vez es más común ver cómo se usa Dropbox o Google Drive para compartir ficheros, lo que además **se ha fomentado gracias a las políticas de BYOD (Bring Your Own Device)**.

La línea que separa el uso de herramientas corporativas de las de uso cotidiano cada vez es más débil y provoca que el mismo procedimiento para compartir una imagen con un amigo o familiar, se use para compartir un documento o una base de datos con un proveedor.

Las organizaciones valoran cada vez más la proactividad, la capacidad de resolución de problemas de manera autónoma. Sin embargo, este comportamiento puede ocasionar problemas, ya que muchos colaboradores acceden a software y aplicaciones para gestión de tarea y de proyectos, agenda, almacenamiento de archivos o cualquier otro tipo de servicio, principalmente **aquellos basados en Cloud, sin el aval y la aprobación del departamento de TI**. Desarrollan el llamado Shadow IT, o TI invisible.

Esto supone un grave problema de privacidad ya que cualquier fallo puede significar la filtración de información confidencial y pérdidas enormes para la organización. Lidar con el Shadow IT es complicado. Según los datos, más del 50% del gasto en tecnología en organizaciones va dirigido al Shadow IT. Esto significa que la mitad de sus presupuestos se gastan en software que los equipos, grupos y unidades de negocios están comprando (y utilizando) sin el conocimiento del departamento de TI.

PROBLEMAS DEL SHADOW IT

Aunque la incorporación de tecnología mediante el modelo Shadow puede ser más ágil, el peligro de hacerlo es alto. Algunos problemas son:

- *Los datos que se envían se almacenan normalmente sin cifrar.*
- *La contraseña utilizada no siempre sigue un criterio de seguridad fuerte.*
- *Las copias de seguridad que se realizan no cumplen la normativa corporativa.*
- *Los datos, una vez enviados, pasan a estar alojados en un proveedor de terceros.*
- *La fuga de datos incumple la GDPR.*

Y es que el Shadow IT permite la apertura de vulnerabilidades para las cuales la infraestructura de tecnología de la empresa no está preparada, por ejemplo:

Pérdida del control. Cuando el departamento de TI no tiene control de una aplicación, la organización tampoco tiene control sobre quién puede acceder a esa aplicación.

Robo de datos. Los propios empleados pueden descargar o robar información, acceder a datos confidenciales o privilegiados simplemente colocando la base de datos de los clientes de la empresa en su Dropbox personal, por ejemplo. También pueden robar datos los ciberdelincuentes, ya que los dispositivos conectados pueden servir como punto de entrada para infiltrarse en una red.

App Sprawl. Término que se utiliza para referirse al uso de muchas aplicaciones diferentes para un mismo fin. La falta de centralización significa un perímetro mucho más amplio, y por ende más difícil de proteger y monitorizar.

Ciberataques. Los empleados pueden instalar contenido con Malware o Ransomware. Los dispositivos conectados vulnerables pueden ser secuestrados o utilizados para expandir la infección al resto de equipos de la empresa.



BOTNETS IOT & DDOS:

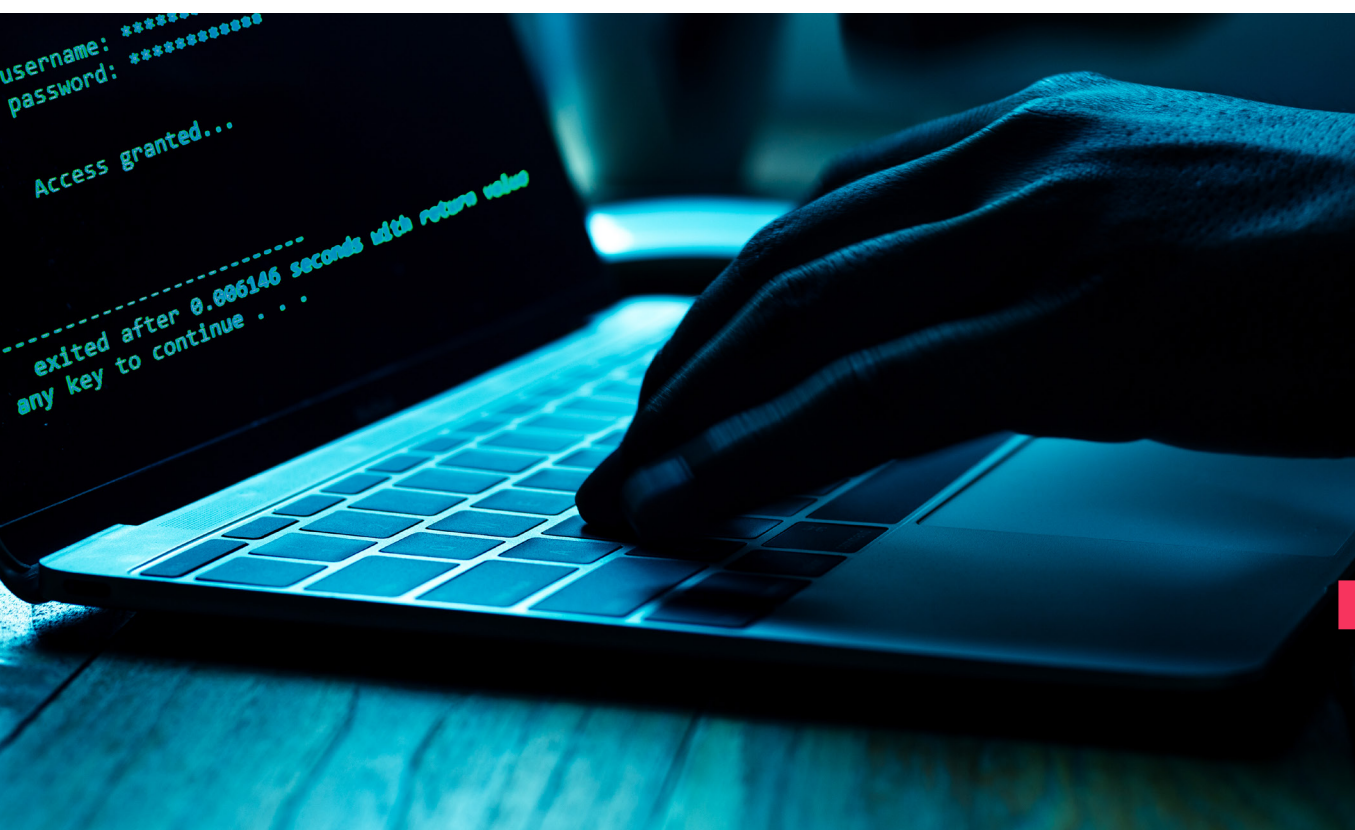
Cada vez hay un mayor número de dispositivos (cámaras, televisores, consolas, aspiradores, etc.) conectados constantemente a Internet, de manera que pueden ofrecer servicio a través de la red y los usuarios controlarlos de forma segura estén donde estén. Sin embargo, este aumento de dispositivos ha ido acompañado de un aumento en el número de Botnets y ataques cibernéticos.

Una Botnet está **formada por un conjunto, generalmente elevado, de dispositivos conectados a Internet que han sido infectados con Malware** y que reciben órdenes de forma remota por parte de los ciberdelincuentes. Los dispositivos infectados que forman parte de una Botnet también se conocen como Bots o zombis.

Cualquier equipo que tenga conexión a Internet, como ordenadores, servidores, routers, dispositivos IoT, cámaras de seguridad, frigoríficos, termostatos, etc., puede infectarse y llegar a formar parte de una Botnet.

Las diferentes tareas que realizan los equipos infectados son dirigidas generalmente desde un servidor central también conocido como C&C (por sus siglas en inglés Command & Control). **Existe otra variedad denominada Botnets P2P** que carecen de ese único servidor C&C debido a la descentralización que proporcionan ese tipo de redes.

El principal problema de las Botnet basadas en dispositivos IoT es que funcionan de manera muy silenciosa. **Se instalan y permanecen inactivas hasta que el servidor central C&C las llama** para realizar una acción. La persona cuyo dispositivo ha sido infectado no notará prácticamente nada, a excepción de que su dispositivo funcionará más lento ocasionalmente.





Este tipo de red generalmente tiene como fin el beneficio económico ilícito de sus creadores. **Para lograrlo pueden utilizar la Botnet de diferentes maneras:**

Ataques de denegación de servicio distribuido o DDoS. El objetivo es impedir el correcto funcionamiento de un servicio, como puede ser la página web de una organización con el consiguiente daño a su imagen y reputación. Para conseguirlo ordenan a un gran nº de dispositivos zombis que accedan a la vez al mismo servicio, haciendo que este se sature llegando incluso a bloquearse e impidiendo que los usuarios puedan utilizarlo. La verdadera novedad es que se ha demostrado que las redes de Bots de IoT pueden atacar a redes eléctricas. Se pueden instalar Botnets en dispositivos IoT de alta potencia, y luego habilitarlos todos al mismo tiempo para provocar un apagón.

Envío de spam. Uso de equipos infectados para enviar e-mails fraudulentos de forma masiva, que en muchos casos incluyen estafas, enlaces a web de Phishing, etc.

Fraudes publicitarios. Normalmente, los servicios de anuncios en Internet pagan a los administradores de las webs donde figuran en función de varios factores, entre los que se incluye la visualización del anuncio y el hacer clic en el mismo. Los ciberdelincuentes ordenan a los Bots que visiten sus propios sitios web y hagan clic en los anuncios para generar beneficios económicos de manera fraudulenta.

Venta y alquiler de la Botnet. Las Botnet en algunos casos son alquiladas por usuarios que desean realizar algún tipo de actividad delictiva, como perpetrar ataques de denegación de servicio. También pueden venderse en porciones para ser utilizados con fines fraudulentos.

Minado de criptomonedas. Las criptomonedas se han convertido en un activo de gran valor, y los ciberdelincuentes pueden utilizar la capacidad de cómputo conjunta de la Botnet para minar criptomonedas sin que los recursos utilizados para ello sean suyos, aumentando de esta forma los beneficios.

Robo de información. La información personal como pueden ser las credenciales de acceso o datos bancarios es valiosa en sí misma, por ello los ciberdelincuentes intentan conseguirla mediante campañas de Phishing lanzadas desde Botnets para posteriormente venderla al mejor postor.

¿CÓMO SE INFECTAN LOS DISPOSITIVOS?

Debido a que los dispositivos de IoT están siempre encendidos, rara vez se monitorizan y suelen usar contraseñas predeterminadas, son blanco fácil para los ciberdelincuentes que buscan formas fáciles de construir un ejército de atacantes maliciosos. Y es que algunos dispositivos como routers y, sobre todo, electrodomésticos, suelen contar con **configuraciones por defecto poco seguras, así como con contraseñas débiles**. Por ejemplo, un frigorífico o un termostato, que rara vez son actualizados o se cambian sus claves. Estas configuraciones débiles son usadas por los ciberdelincuentes para obtener acceso y convertirlo en parte de la Botnet.



DEEP WEB, DARK WEB & DARKNET:



Deep Web :

Se trata de todo ese espacio digital que se encuentra al margen de la Clearnet: toda la parte de Internet a la que cualquier internauta puede acceder fácilmente desde cualquier navegador (páginas web indexadas en buscadores, sitios ubicados en la World Wide Web, páginas públicas de las RR.SS, etc.) y en la que cualquier usuario puede ser rastreado fácilmente mediante su dirección IP. La Deep Web **engloba toda esa información que está alojada online, pero a la que no se puede acceder de forma pública.** La Deep Web también la componen sitios con un disallow en el archivo robots.txt o las páginas dinámicas que se generan al consultar una base de datos.



Dark Web:

La Dark Web incluye todo ese espacio de Internet al que únicamente se puede acceder a través de aplicaciones específicas. Así como la Deep Web supone en torno al 90% de del contenido de la World Wide Web, la Dark Web ocuparía únicamente el 0,1% de ella. **Engloba todo el contenido que ha sido ocultado de forma deliberada.** Es conocida por su uso como mercado negro digital para el tráfico de contenidos ilegales, así como la difusión de actividades delictivas. También es considerado como un espacio anónimo que permite la privacidad en línea y la seguridad de las comunicaciones digitales, protegiendo a los usuarios de la vigilancia masiva y la censura.



Darknets:

Por último, las Darknets son redes específicas, como TOR o I2P (las más populares), que están construidas para alojar aquellas páginas que se quieren ocultar. **Muchas de las Dark Webs que están alojadas en estas plataformas tienen fines altamente delictivos.**

Pero, aparte de estas conocidas actividades ilícitas, las Darknets también son habitualmente empleadas por los ciberdelincuentes para perpetrar ataques. Según varios estudios, entre los años 2016 y 2019 se produjo un incremento del 20% en el número de Darknets listadas con potencial peligro de causar incidencias de Ciberseguridad en las organizaciones.

Entre estos peligros se incluían alojamiento de Malware, comercialización de servicios DDoS específicos para ciberataques a empresas, venta de datos corporativos privados robados, venta de contraseñas robadas y difusión y venta de herramientas de Phishing y extorsión digital a empresas.

Las investigaciones revelan también que en el 40% de las Darknets se están vendiendo servicios de hacking específicamente diseñados para atacar a importantes empresas de Fortune 500 o FTSE 100.

Por tanto, los cibercriminales más experimentados se sirven a menudo de las Darknets para mantener el anonimato y protegerse de que su rastro sea detectado. Allí pueden tanto encontrar herramientas para perpetrar sus ataques como ganar dinero vendiéndolas a otros delincuentes.



¿Cómo proteger los datos?

04

Actualmente, **el 75% de los equipos de IT declaran que la Ciberseguridad supone un desafío esencial para sus compañías**. Los principales retos son la captación de talento y el presupuesto, que en muchas ocasiones conllevan un avance más lento de las empresas respecto a los ciberdelincuentes, cuyos métodos de ataque no paran de evolucionar. Los directores de IT utilizan de media el 26% de su tiempo en el ámbito de la Ciberseguridad, aunque 8 de cada 10 declaran que el equipo con el que cuentan no es suficiente para hacer frente a las amenazas, y el 70% indica que la inversión por parte de la empresa no es suficiente para situarse a la altura en infraestructuras, tecnología y formación, para responder adecuadamente a los ciberriesgos.

En este contexto, cabría pensar que el principal vector de ataque es un conjunto de sofisticados Malware que infectan los equipos de las empresas, pero no es así: el principal punto de entrada de los ciberdelincuentes son los empleados, a través de la ingeniería social. Contactan con ellos a través de correo electrónico o redes sociales, suplantando la identidad de una entidad de confianza. Tarde o temprano, provocan que el empleado ejecute algún tipo de Malware, o introduzca sus datos privados en algún entorno falsificado (Phishing).





Aunque las soluciones antivirus son parte esencial de la política de seguridad, su naturaleza es reactiva, pues se centran en la detección y desinfección. Las empresas deben **desarrollar políticas preventivas, de alerta temprana, para evitar que la infección llegue a producirse.**

Estas estrategias tienen una parte tecnológica, como por ejemplo las infraestructuras de seguridad que conectan a todos los equipos de la compañía entre sí, para evitar que se extienda la infección una vez detectada en un solo equipo; pero también tienen una parte puramente formativa: la cultura de la desconfianza. Se trata de formar a los empleados para que desconfíen sistemáticamente, se familiaricen con los distintos tipos de ataques y ejecuten solo las acciones de las que están totalmente seguros.

Por otra parte, los sistemas de seguridad deben **ofrecer una protección enfocada al endpoint.**

Para proteger realmente los datos y sistemas de la empresa, la Ciberseguridad debe focalizarse en el dispositivo final utilizado por cada empleado. Los perímetros de seguridad tradicionales han terminado por difuminarse gracias a la multiplicidad de dispositivos y canales, y la movilidad que ello permite, por lo que las políticas de Ciberseguridad no pueden dirigirse a establecer un perímetro, sino a proteger el dispositivo final.

En este sentido, **las tablets y Smartphones son cada vez más el objetivo de los ciberataques, pues se accede frecuentemente desde ellos a los entornos corporativos y almacenan datos sensibles.**

Además, un archivo infectado que afecte a un móvil puede expandirse con relativa facilidad a los equipos PC. Por ello es necesario extender la política de seguridad a todo tipo de dispositivos, máxime cuando los empleados utilizan cada vez más sus propios dispositivos personales para conectarse.

Además, la tecnología abre la posibilidad del trabajo remoto, diluyéndose la diferencia entre el trabajo en las instalaciones de la empresa y el trabajo desde cualquier otra ubicación o dispositivo. **Es fundamental establecer una política de seguridad y protección de datos en este entorno deslocalizado.** Para ello, es una buena opción la conexión remota, de modo que el equipo del usuario se conecte al equipo de la empresa, evitando acumular datos y credenciales sensibles en dispositivos personales. Asimismo, es esencial que las comunicaciones se realicen a través de una VPN (Virtual Private Network), para cifrar el tráfico entre dispositivos y evitar cualquier acceso no autorizado a la red y a los datos.



Existen gran cantidad de medidas, tanto tecnológicas como de gestión, que deben aplicar las organizaciones para evitar ser víctimas de ciberataques:

Determinar los datos que se almacenan.

Es esencial realizar una auditoría de todos los datos, identificar cuáles son de dominio público y cuáles son datos personales o claves para el negocio. Solo desde el mapeo claro de los mismos es posible establecer políticas de protección adecuadas, con medidas más estrictas y derechos de acceso restrictivos.

Usar múltiples métodos de autenticación.

Las contraseñas no son suficientes por sí mismas en muchos casos, por lo que es cada vez más popular el uso de múltiples factores, como el envío de un código vía SMS o la biometría para el reconocimiento facial o de la huella dactilar.



Habilitar el protocolo HTTPS.

El certificado SSL/TLS garantiza que los datos transmitidos entre el navegador y el servidor están cifrados, protegiéndolos frente a posibles intrusiones de terceros. Estos protocolos verifican la identidad del servidor, esencial para evitar el Phishing. Muchas organizaciones configuran sus equipos para que solo permitan acceder a páginas con certificado SSL.

Realizar copias de seguridad.

Muchos ciberataques persiguen el robo o destrucción de los datos, lo que puede generar pérdidas económicas millonarias en una organización. Es esencial que se realicen periódicamente copias de todos los datos sensibles y se almacenen en entornos seguros, separados física y virtualmente de los equipos que intervienen en la operativa diaria.

Uso de contraseñas sólidas y únicas.

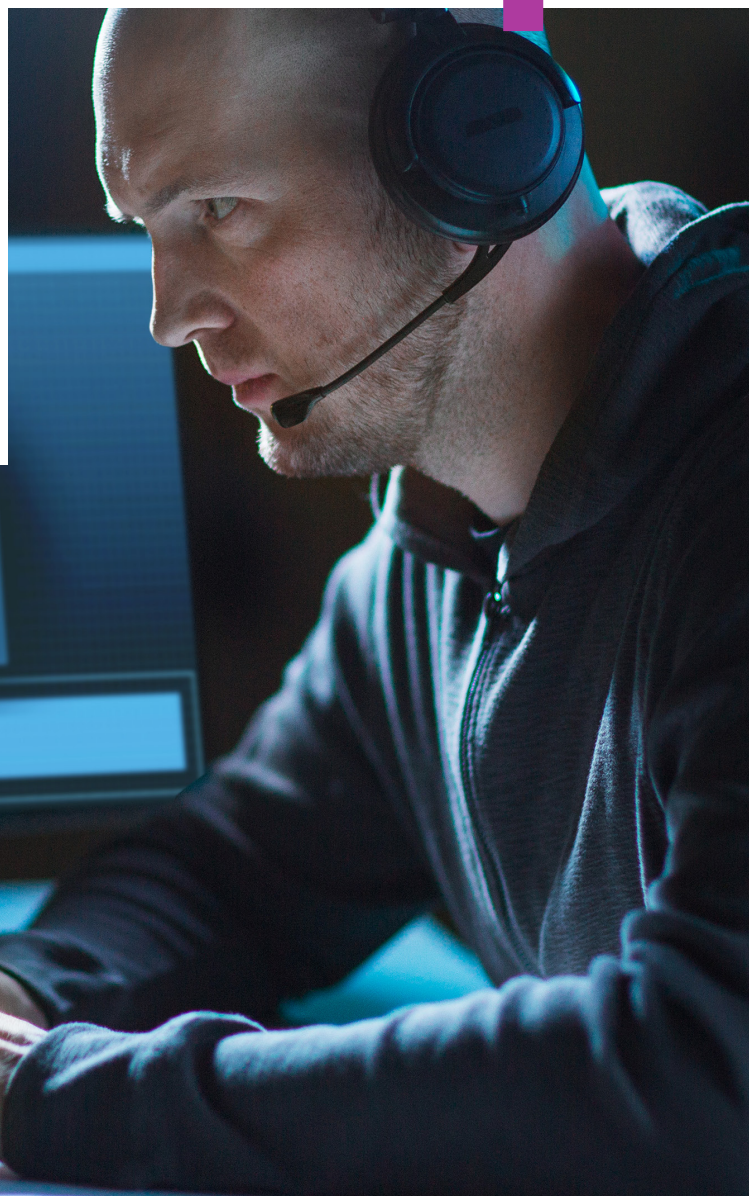
Si el usuario utiliza la misma contraseña para todas sus cuentas, la sustracción de la misma en un único entorno permite el acceso a las plataformas empresariales a las que tiene acceso el empleado. Es recomendable utilizar un gestor de contraseñas, que genere automáticamente claves seguras y las almacene para evitar que sean olvidadas.

Establecer una política de uso de dispositivos propios.

Dotar a los empleados de formación para el acceso al entorno empresarial desde sus móviles o tablets, y el diseño de una política adecuada para la protección de estos dispositivos son medidas esenciales. Se trata de evitar que los dispositivos de los empleados sean utilizados como puntos de acceso a la red corporativa.

Mantener actualizado el software.

Las compañías de desarrollo tratan de detectar todas las posibles vulnerabilidades de sus programas, y crear parches que las solventen con la mayor brevedad antes de que sean aprovechadas por ciberdelincuentes. Si no se garantiza que todo el software de la empresa utilice la última versión, es más probable que se halle la forma de acceder ilícitamente a los sistemas.



Habilitar comunicaciones seguras a través de correo electrónico.

Para evitar la revelación de datos y los ataques de Phishing, es importante utilizar herramientas para cifrar los mensajes en tránsito y verificar su origen.

Simular ataques de Phishing.

Muchas organizaciones realizan pruebas de simulación para comprobar el grado de alerta de los empleados, y detectar las necesidades formativas del personal.

Análisis de amenazas internas.

Este tipo de estudios revelan las amenazas contra la infraestructura informática procedente del interior de la compañía. Los puntos débiles pueden ser un empleado, proveedor o colaborador.

Crear directrices de respuesta rápida.

Se trata de prepararse para responder de forma rápida frente a un ciberataque. El plan debe ser conocido por el conjunto de la organización, y debe designarse a un responsable para su ejecución.

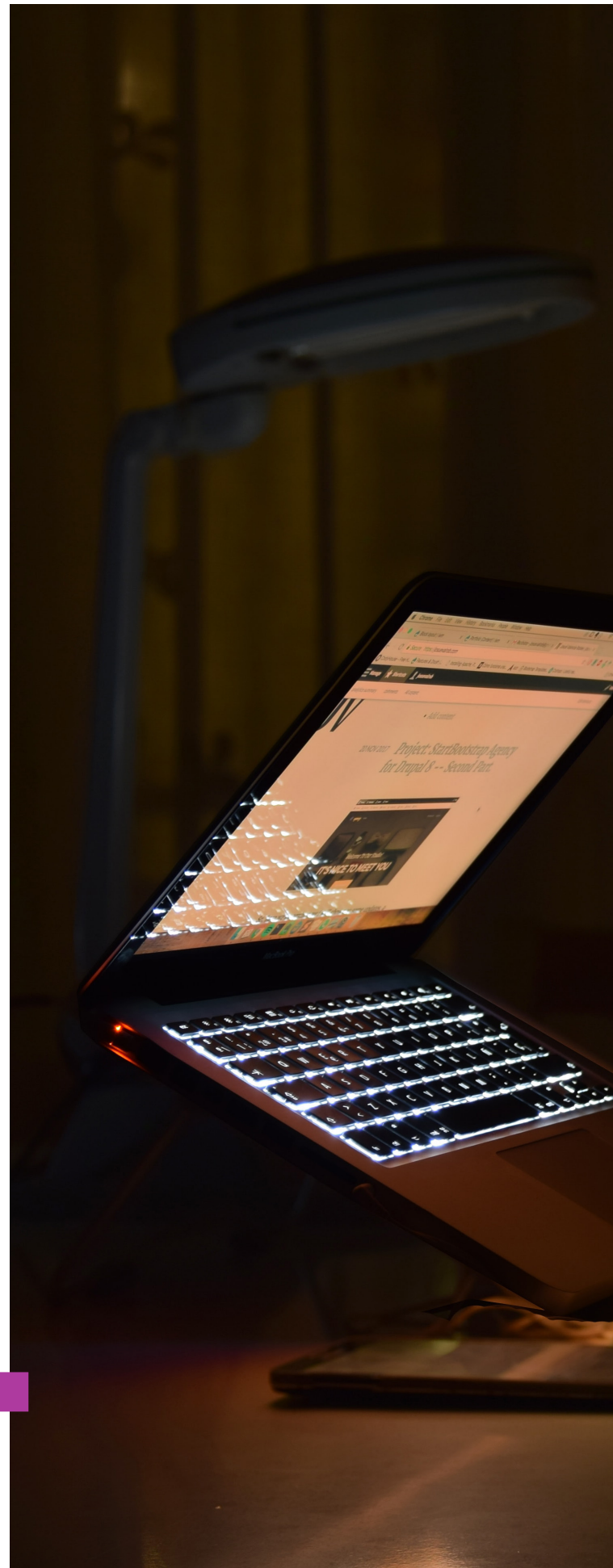
Suscribir un ciberseguro.

Las pérdidas materiales y reputacionales que puede ocasionar un ciberataque revisten un inmenso valor. Es fundamental que las organizaciones aseguren sus infraestructuras, sus bases de datos y su identidad digital.

Segmentar la red. Es necesario evitar que la totalidad de la red informática sea accesible desde un mismo punto. Es necesario separar las infraestructuras físicamente, y sobre todo a nivel de arquitectura de red, para dividir los sistemas según su importancia y aplicar medidas de seguridad adaptadas.

Borrar de forma segura la información.

Cuando los ficheros o datos son eliminados de un equipo, su rastro permanece en el disco duro, lo que los hace recuperables. Esto entraña importantes peligros de cara a posibles ciberataques, por lo que es recomendable usar herramientas específicas de borrado de datos, que sobrescriben el fragmento de memoria con cadenas aleatorias.

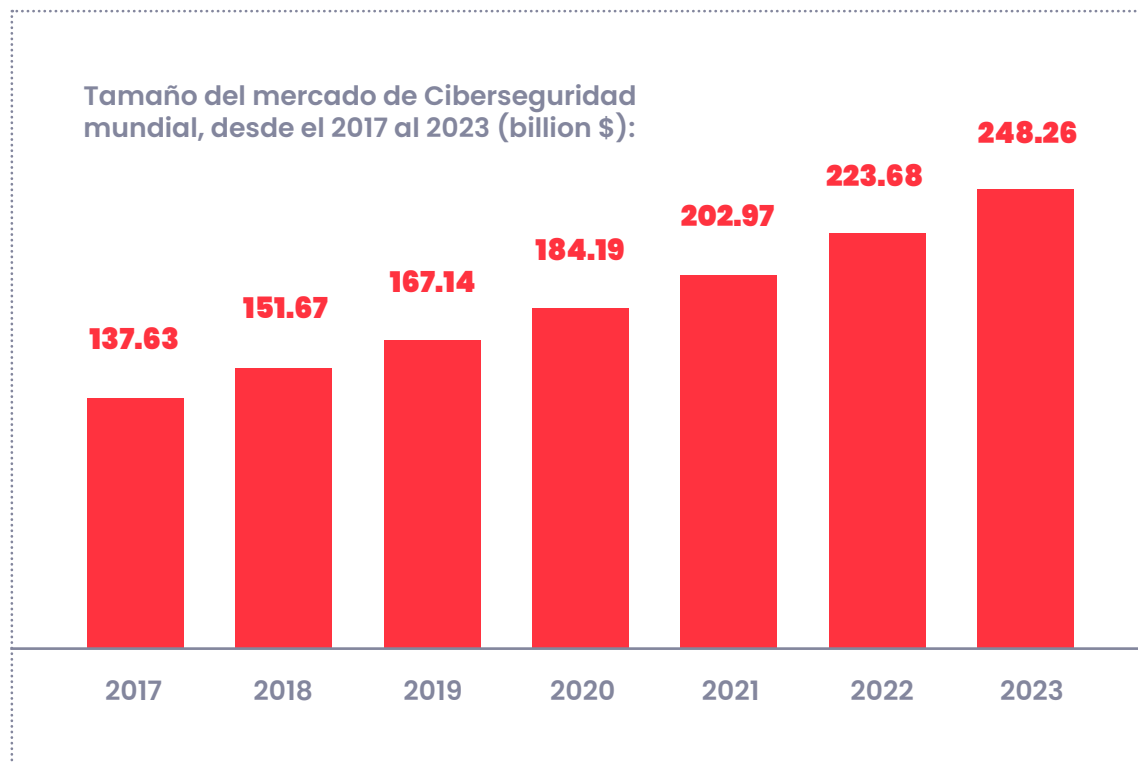




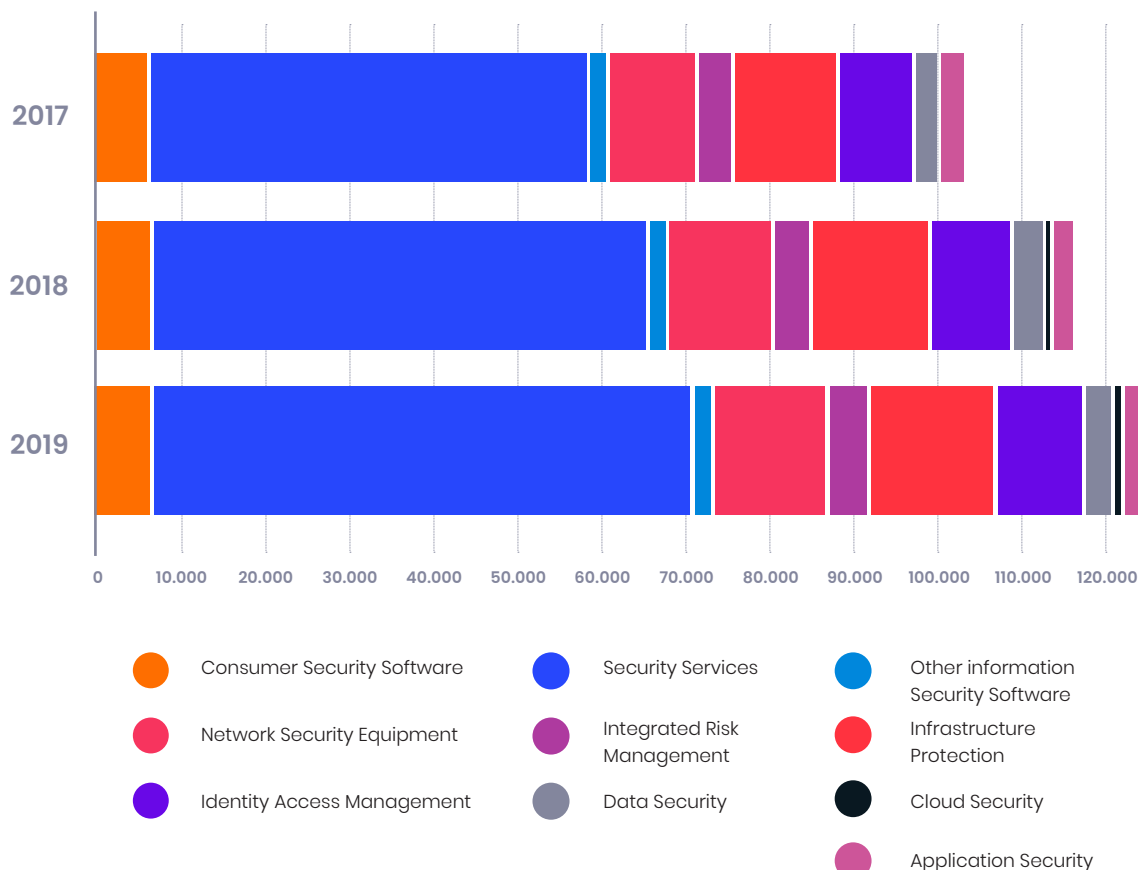
Nuestras Conclusiones

El mercado global de la Ciberseguridad ha crecido desde 137.000 millones de dólares en 2016, hasta los 167.000 millones actuales, aunque su crecimiento es exponencial, y lejos de estar moderándose (como sucede con la mayor parte de áreas tecnológicas con un elevado grado de madurez en la adopción), **está acelerándose, hasta el punto de que se prevé que alcance los 248.000 millones a partir de 2023.**

Por otra parte, la inversión de las empresas en Ciberseguridad se distribuye en varios conceptos, entre los cuales **destacan los servicios externos de seguridad, que acaparan el 50% del gasto.** También son áreas relevantes de gasto las aplicaciones de Ciberseguridad, la gestión de la identidad, la protección de infraestructuras o el equipamiento de seguridad de redes, que alcanzan conjuntamente una cifra todavía inferior a los servicios externos de Ciberseguridad. Llama la atención, en cualquier caso, que el gasto en seguridad de los datos y en seguridad Cloud solo ocupen el 5% del gasto total, aunque se prevé que aumente significativamente en los próximos años, teniendo en cuenta la adopción acelerada de los entornos Cloud por prácticamente la totalidad de grandes empresas.



Gasto mundial en Seguridad de la Información desde 2017 a 2019 (million \$) por segmento:



Existen otros indicadores que revelan la creciente pero todavía insuficiente apuesta de las empresas por la Ciberseguridad, teniendo en cuenta la gravedad de los potenciales ataques: **el presupuesto específico para Ciberseguridad apenas supera el 10% del presupuesto total de los departamentos IT**, y de los 167.000 millones de dólares que gastan las empresas en Ciberseguridad, más de la mitad se dirigen a la protección de entornos PC, aunque cada vez se concede más importancia a los dispositivos IoT, aumentando la inversión para protegerlos hasta los 30.000 millones en 2019.

Las cifras de inversión contrastan con la de los ciberataques:

2.000 millones más en 2018 que en 2017. Y aunque la mayoría continúan siendo ataques tradicionales normalmente de baja sofisticación (el 13% son downloaders, el 10% RATs y el 8% webshells), crecen los nuevos ataques, como los coin miners, el 3% del total, y los memory scraper, el 8% del total. Por lo que al Ransomware se refiere, su popularidad ha disminuido considerablemente, desde los 638 millones de ataques en 2016 a los 204 millones en 2018, esto es, el 0,7% del total de ciberataques. Aun así, los robos de datos están a la orden del día: 3.000 millones de registros a Yahoo, 2.200 millones a Facebook, 885 millones a First American Financial Corporation, 330 millones a Twitter, e incluso 198 millones a la base de datos de votantes de Estados Unidos, por poner solo algunos ejemplos.



Por su parte, el impacto económico de los ciberataques en las empresas es cada vez mayor: se calculan de media 27,37 millones por empresa en concepto de pérdidas en Estados Unidos. El norteamericano es sin duda el mercado más afectado por los ciberataques. Por poner un ejemplo, el 30% de los ataques DDoS se dirigen contra empresas de dicho país, solo compitiendo con el área Asia-Pacífico. No obstante, cabe señalar que Europa y Oriente Medio fueron víctimas del 27% de los robos de datos que tuvieron lugar en 2018.

La ciberdelincuencia es un problema de alcance global, con un impacto económico y reputacional extraordinariamente relevante para las empresas, y cuya complejidad y sofisticación es cada vez mayor, conforme avanzan las técnicas de hacking, y las empresas cuentan con más dispositivos (la irrupción del IoT es el caso más evidente de este fenómeno). La Ciberseguridad perimetral, propia de un paradigma tradicional en que era suficiente con proteger los equipos de la empresa, ha muerto a causa de la emergencia de los entornos abiertos: empresas que integran sus sistemas con proveedores y usuarios, almacenan sus datos en la nube, etc.

El reto de las empresas pasa ahora por **trazar un plan estratégico de Ciberseguridad**, que conjugue coherentemente la inversión en tecnología, la captación de talento capaz de gestionar un entorno altamente complejo de infraestructuras, y la formación del personal en la materia. Este último factor es clave, pues ni la más sofisticada de las herramientas de Ciberseguridad puede paliar totalmente los efectos de un personal vulnerable a la ingeniería social de los ciberdelincuentes.





**Somos expertos en servicios,
productos y soluciones digitales,
en innovación tecnológica y en
procesos ágiles de transformación.**

Con un equipo humano de **más de 2.500 profesionales**, tenemos presencia a nivel nacional e internacional, con sedes en EE. UU., Perú, Brasil, Chile, México, Colombia, Paraguay, Reino Unido y Alemania.

¿Nuestra misión? Generar el mayor valor a nuestros clientes, a los sectores económicos y al conjunto de la sociedad, mediante el diseño y desarrollo de iniciativas **basadas en tecnología de vanguardia**, con el objetivo de accionar el cambio digital de una manera disruptiva.

www.vectoritcgroup.com

