ESPECIAL

“Hack&News”

DE Tecnología & Sentido Común

AGOSTO
2021

ESPECIAL "Hack&News" DE Tecnología & Sentido Común

EQUIPO DIRECTO:
Javier Peris - Piloto
Manuel D. Serrat - Copiloto
Alberto Rodríguez - Equipo Directo
Juan Carlos Muria - Equipo Directo

MICRO-ESPACIOS
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Catalina Valencia - Ecosistema Emprendedor
Víctor Almonacid - La Nueva Administración
Shirley Villacorta - América Próxima
Fernando Ley - Geo Energía

PUBLICIDAD Y CONTRATACIÓN
Carmen Usagre
carmen.usagre@businessandcompany.com
Teléfono: +34 96 109 44 44

GABINETE JURÍDICO
Jesús López Peláz

ATENCIÓN AL LECTOR
tecnologiaysentidocomun@businessandcompany.com

EDITA
Business, Technology & Best Practices, S.L.

Av. San Onofre, 20
46930-Quart de Poblet (Valencia)
Teléfono: 96 109 44 44
Fax: 96 109 44 45
https://businessandcompany.com
soluciones@businessandcompany.com

ALBERTO RODRÍGUEZ

ITIL Expert, Consultant Manager de ISO/IEC 20000, Certificado en Gestion de Proyectos con PRINCE2 y por supuesto en COBIT5. Ha trabajado en proyectos con la administración pública como desarrollador y analista de procesos de TI, con operadores de comunicaciones a nivel nacional, en diversos proyectos de concienciación en ciberseguridad. Es miembro de la organización de RootedCON que organiza uno de los congresos de seguridad informática más importantes a nivel nacional y europeo. Junto con el equipo de RootedCON organizan el evento más importante relacionado con Seguridad de la Información de cuantos se llevan a cabo en Valencia "RootedValencia""

LinkedIn:
https://www.linkedin.com/in/arodriguezp/

Twitter:
https://twitter.com/albert0r

PREPARA A TU ORGANIZACIÓN PARA RETOS FUTUROS CON ITIL® 4

Los avances tecnológicos han transformado la forma en la que adquirimos e interactuamos con bienes y servicios; creando nuevos comportamientos, expectativas y experiencias.
Pero ¿estás preparado para esos retos?

El mundialmente reconocido ITIL 4, es el método de gestión de servicios que proporciona, a organizaciones y profesionales, un modelo operativo digital / de TI de extremo a extremo para la entrega y operación de productos y servicios habilitados por tecnología y permite a los equipos de TI continuar desempeñando un papel crucial en una estrategia de negocios más amplia.

¿Quieres conocer más?

AXELOS.com/ITIL4-futuro
(Página en inglés)

ESPECIAL AGOSTO 2021

TECNOLOGIA Y SENTIDO COMUN #TYSC

índice
DE CONTENIDOS

https://tecnologiaysentidocomun.com

Índice de Contenidos

¡ic

#TYSC

Más problemas en la época post-covid

AL SER UN TEMA DE ACTUALIDAD Y COMO NO PODÍA SER MENOS, EN ÉSTE PRIMER NÚMERO DE LA NUEVA REVISTA TECNOLOGÍA Y SENTIDO COMÚN, VAMOS A HABLAR DE LA "NUEVA NORMALIDAD" QUE ESTAMOS VIVIENDO DENTRO DEL MARCO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN.

Una "nueva normalidad presidida por una transformación digital sobrevenida, donde la mayoría de las empresas han tenido que implantar a contrarreloj y de forma obligada los medios para garantizar a sus emplea- dos la accesibilidad al trabajo remoto.

Si algo hemos observado, es que no estamos preparados para afrontar de forma segura una situación tan compleja como la vivida. Por ejemplo: mediante la utilización de conexiones poco seguras, uso del equipamiento de los propios empleados, infraestructuras que no están preparadas para soportar el tráfico o falta de securización de las aplicaciones corporativas son algunos de los problemas que llegan con esta nueva situación.

¿Qué implica todo esto?

Los ciberdelincuentes han encontrado de forma fortuita un nuevo nicho y que según datos de IBM los ciberataques han aumentado un 125% en Europa durante el primer trimestre de 2020 y un 40% a nivel mundial durante la pandemia. Los ciberdelin- cuentes no han parado, y han aprovechado esta situación para lanzar ataques con la finalidad de robar datos, infectar dispositivos y realizar transacciones bancarias fraudulentas.

Como todos sabemos si ya es difícil que los CIO s / CISOS s protejan los datos de sus corporaciones en una situa- ción normal, imaginemos la cantidad de dificultades que tienen a la hora de proteger los activos de la empresa cuando éstos se distribuyen en equipos domésticos.

Los principales ataques que se han sufrido durante estos meses se centran principalmente en campañas de phishing, la mayoría explotando la COVID-19 y suplantando a organizaciones como la OMS.

En otras ocasiones, los atacantes proponen al receptor de los mensajes colaborar en la recaudación de fondos contra el virus, haciéndole participe de un fraude.

Otro de los vectores de ataque que más han proliferado es la instalación de malware en dispositivos, mediante la descarga de aplicaciones que ofrecen cupones de descuento de restaurantes, supermercados, etc. dejando el dispositivo bajo el control de los atacantes además del acceso a datos sensibles.

CONTINÚA EN PRÓXIMA PÁGINA

Así mismo, a mediados de septiembre se publicó una nueva vulnerabilidad en Windows Server, cata- logada por el NIST con una criticidad de 10/10. Dicha vulnerabilidad afecta de forma directa a los controladores de dominio del Directorio Activo debido a un error de implementación criptográfica del protocolo Netlogon, que permite reestablecer una contraseña y hacerse con el control del Domain Controller (CVE-2020-1472).

Aunque el pasado mes de agosto Microsoft lanzó una serie de parches oficiales, aún no se han publicado medidas alternativas en caso de no ser posible aplicar los mismos y habrá que esperar al mes de febrero a que se publiquen nuevas actualizaciones que tratarán de mitigar esta vulnerabilidad.

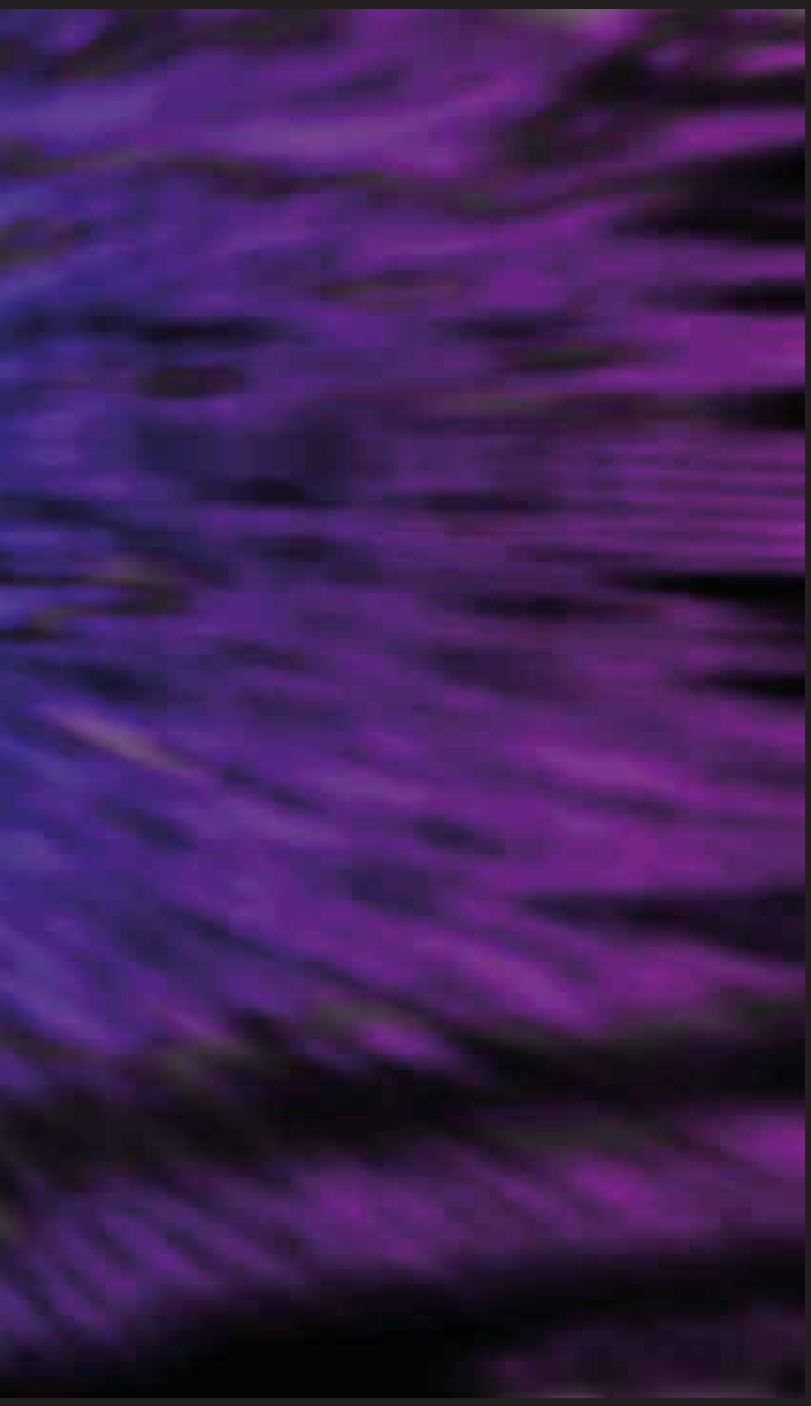
Pese a que el año 2020 está siendo un cúmulo de circunstancias, tenemos la oportunidad y la obligación de demostrar que con esfuerzo e inversión, podemos proteger los activos y datos de las compañías. Para ello es vital la suma de esfuerzos.

Vulnerabilidades en las empresas y cazadores de bugs.

Sabemos que una vulnerabilidad, en términos informáticos, es un fallo en un sistema de información que pone en riesgo la seguridad, integridad, confidencialidad o disponibilidad de la información que poseen o con la que trabajan las empresas.

Para detectar y corregir las vulnerabilidades en sus sistemas las empresas auditan sus sistemas de forma exhaustiva mediante diferentes tipos de monitorización y controles que permite detectarlas.

> **Una nueva forma de hacking ético ha llegado y ha venido para quedarse.**



Todos los lectores conocemos que este tipo de auditorías tienen un alto coste, pero desde un tiempo hacia acá ha aparecido un nuevo perfil dentro del área de la ciberseguridad que se centra en este tipo de amenazas: los cazadores de bugs. Empresas de la talla de Google, Microsoft, Facebook, Apple, cuentan con programas de Bug Bounty que ofrecen no sólo recompensas de tipo económico, sino también reconocimiento a todas aquellas personas que encuentren vulnerabilidades en sus sistemas o productos. Son programas totalmente abiertos que ayudan a detectar y corregir fallos que pueden poner en peligro tanto su propia seguridad como la seguridad de los usuarios que utilizan sus productos.

Estas compañías, ponen a disposición de los expertos en seguridad informática o de cualquier persona que quiera incrementar su experiencia dentro del hacking ético, el o los productos sobre los que quieren realizar análisis de vulnerabilidades. Una vez en dichas plataformas los investigadores intentan descubrir fallos o errores por las que son pagados en base a la criticidad de los mismos.

CONTINÚA EN PRÓXIMA PÁGINA

Uno de los programas más conocidos sobre Bug Bounty es el llamado “Hack the Pentagon”, programa en el cual el Departamento de Defen- sa de los Estados Unidos pagó más de 70.000$ a diversos investigadores por numerosos bugs encontrados.

El mercado de los Bug Bounty en España es un mercado que está aún por explotar. Esto se debe en parte a las dudas que tienen las empresas españolas ante este tipo de plataformas. En otros países de Europa y América, plataformas como la conocida Yogosha o HackerOne se abren paso dentro del mercado de la ciberseguridad con este novedoso producto.

Tal es el cambio que se propone con este nuevo formato que, la división de seguridad de Telefónica Tech, Eleven Paths, se plantea usar este tipo de auditoría/pentesting para ofrecerlo a sus clientes de forma privada y de esta forma abrir un poco más este mercado dentro del territorio nacional.

Este amplio abanico de posibilidades que se abre, permite a analistas de seguridad con una amplia experiencia probar los sistemas y productos de grandes multinacionales, reduciendo de forma considerable la posibilidad de que un bug sea pasado por alto.

Con esta nueva forma de “responsible disclosure” muchos expertos en seguridad de la información, que hasta ahora veían que reportar de forma directa a la empresa les podía suponer un problema legal, se animarán a enviar los fallos que encuentren amparándose en el paraguas que les ofrecen las empresas especializadas.

Una nueva forma de hacking ético ha llegado de la mano de este tipo de empresas y ha venido para quedarse.

más información en:
https://javierperis.com/bpm

Y tú ¿Transformas o Trastornas tu Organización?

Aprende a:

- ✓ Modelar
- ✓ Mejorar
- ✓ Automatizar Procesos de Negocio

Curso Oficial de Certificación en
Gestión de Procesos de Negocio
ISO/IEC 19510
BPM Professional

Si quieres Aprender, Certificarte, Practicar y recibir posteriormente Ayuda para Liderar con Éxito la Transformación Digital en tu Departamento, Startup, Empresa o Administración, no te quede la menor duda de que este es tu Curso y esta es tu Certificación.

Business&Co.®
Business, Technology & Best Practices, S.L.

Phishing, vishing, y smihing

Como ya sabemos, los ciberdelicuentes, (por desgracia,) van casi siempre un paso por delante de lo que a seguridad defensiva se refiere.
En este número vamos a hablar de ataques en los que prima sobre todo la ingeniería social y que utilizan al eslabón más débil de la cadena, el usuario, para conseguir su finalidad, que en la mayor parte de los casos suelen ser credenciales de acceso a todo tipo de servicios, correo, ocio, banca, o acceso a cualquier otro tipo de datos de carácter personal.
El más conocido de estos ataques, por su antigüedad es el phishing, un ataque que suele ser realizado a través del

correo electrónico, y que con un coste de ejecución muy bajo produce a los atacantes beneficios muy elevados.
Aunque la mayor parte de campañas de *phishing s*e basan en enviar correos electrónicos masivos a la mayor cantidad posible de personas nos encontramos también con ataques dirigidos a empresas o personas concretas, esto es lo que llamamos *spear phishing*. Habitualmente se ataca con un tipo de contenido personalizado, lo que requiere un conocimiento previo del objetivo anterior a la realización del ataque, generando de esta forma un correo atractivo y creíble para la víctima. Este tipo de ataque es una de las amenazas consideradas críticas para corporaciones empresariales y gobiernos y supone una cantidad muy elevada de dinero perdido anualmente.

Otro de los ataques que en la actualidad los ciberdelincuentes están utilizando es el *phishing* telefónico o *vishing*. Este fraude consiste en una suplantación de identidad utilizando la voz y suplantando a bancos, policía, o incluso a la Agencia Tributaria.
Intenta convencer a la víctima de que tiene algún tipo de problema y le solicita datos de carácter personal, como número de cuenta bancaria, o número de tarjeta de crédito, instando a la víctima a efectuar algún tipo de pago mediante transferencia o incluso mediante tarjetas prepago debido a la dificultad de rastreo que presentan las últimas.
Otro de los ataques de vishing que más proliferan es el del soporte técnico de Microsoft en el que el atacante se ofrece a "ayudar" a la víctima a solucionar algún tipo de problema existente en su equipo informático, para de esta forma tomar el control del mismo y acceder a datos, principalmente de tipo económico. Destacar también la insistencia de los atacantes en las víctimas, habiendo llegado a contar hasta seis llamadas telefónicas en el mismo día con la finalidad de convencer al usuario atacado de la gravedad de su problema.
Este tipo de fraude va avanzando tecnológicamente, incorporando inteligencia artificial que es capaz de suplantar la voz de las personas y contactando con los departamentos de administración o contabilidad de las compañías con lo cual en muchas ocasiones es difícil de identificar. ¿Quién le dice al CEO de su propia empresa, al que está escuchando por teléfono que no va a hacer la transferencia que le está solicitando?
Es muy importante concienciar a todos los empleados de la compañía de la existencia de este tipo de ataques e implantar medidas que impidan o en su defecto dificulten el éxito de este tipo de ataques. No es necesario mencionar que el daño económico que implica en las empresas es uno de los más altos, ya que las cantidades suelen ser bastante elevadas.
Por último, siguiendo este paseo por los diferentes tipos de suplantación de identidad, nos encontramos con el smishing. Otro tipo de phishing, pero esta vez utilizando los mensajes sms como método de engaño.
A menudo suele suplantar la identidad de un banco y busca información de tipo personal o financiero.
El atacante utiliza la confianza que la víctima deposita en el teléfono móvil, ya que muchos usuarios lo consideran más seguro que el ordenador, sin ser conscientes de que la seguridad que el teléfono móvil presenta frente a este tipo de ataques es bastante escasa.

CONTINÚA EN PRÓXIMA PÁGINA

A medida que más personas usan sus propios terminales móviles para trabajar el smishing se está convirtiendo en una amenaza bastante seria a nivel empresarial. El lado bueno de este tipo de ataque es que es relativamente fácil protegerse del mismo, de hecho como más protegido se está es sin hacer nada. Este tipo de ataques sólo pueden ocasionar daños o pérdidas si la víctima "muerde" el anzuelo. Consejos como tener claro que nuestra entidad bancaria nunca nos va a solicitar actualizar información sobre nuestra cuenta, o no hacer click en enlaces acortados pueden suponernos la diferencia entre ser o no víctimas de este tipo de ataques.

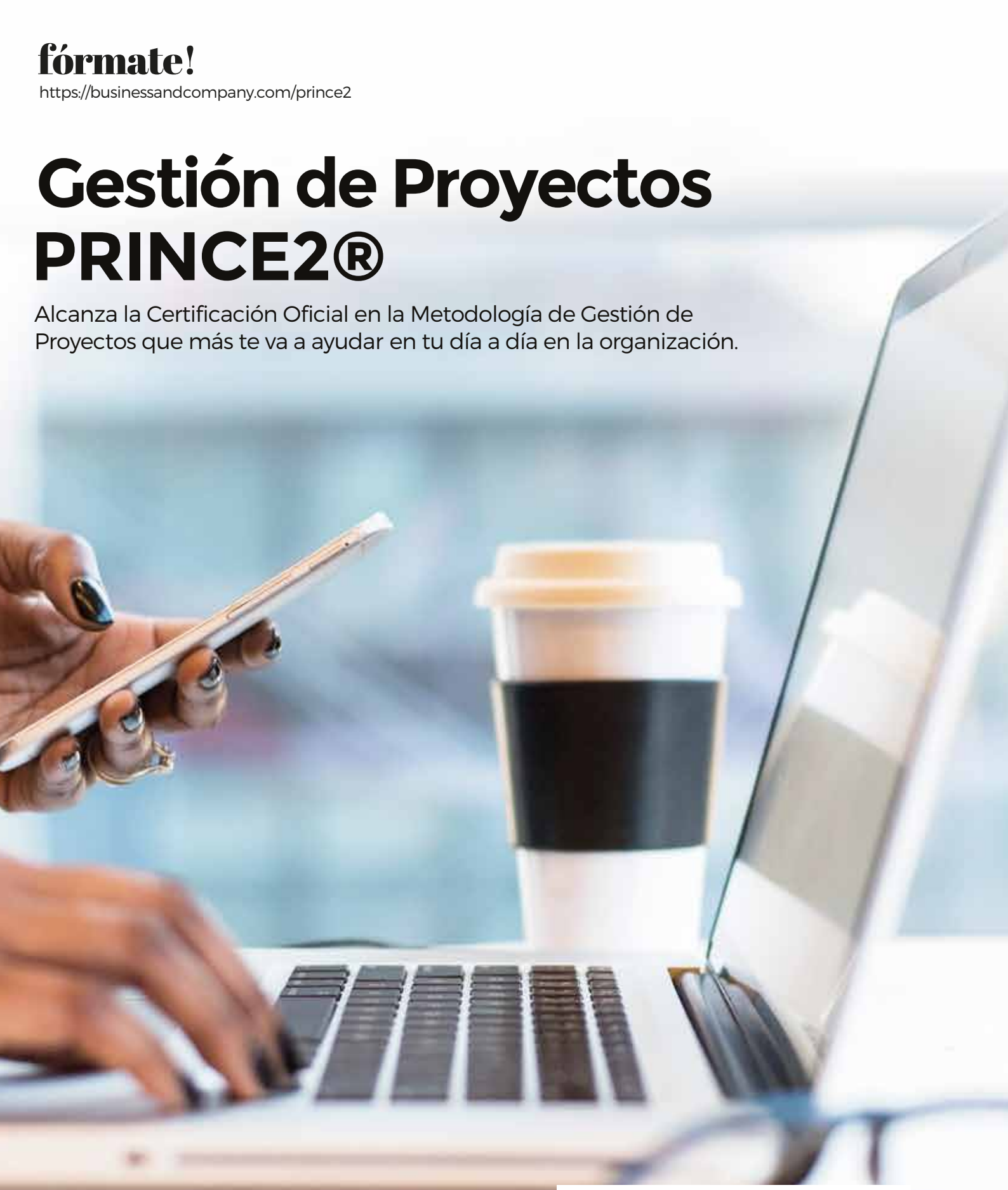
Como en la mayoría de los tipos de ataque por suplantación de identidad el sentido común es parte fundamental de la protección ante los mismos.

fórmate!

https://businessandcompany.com/prince2

Gestión de Proyectos PRINCE2®

Alcanza la Certificación Oficial en la Metodología de Gestión de Proyectos que más te va a ayudar en tu día a día en la organización.



Business&Co.®
Business, Technology & Best Practices, S.L.

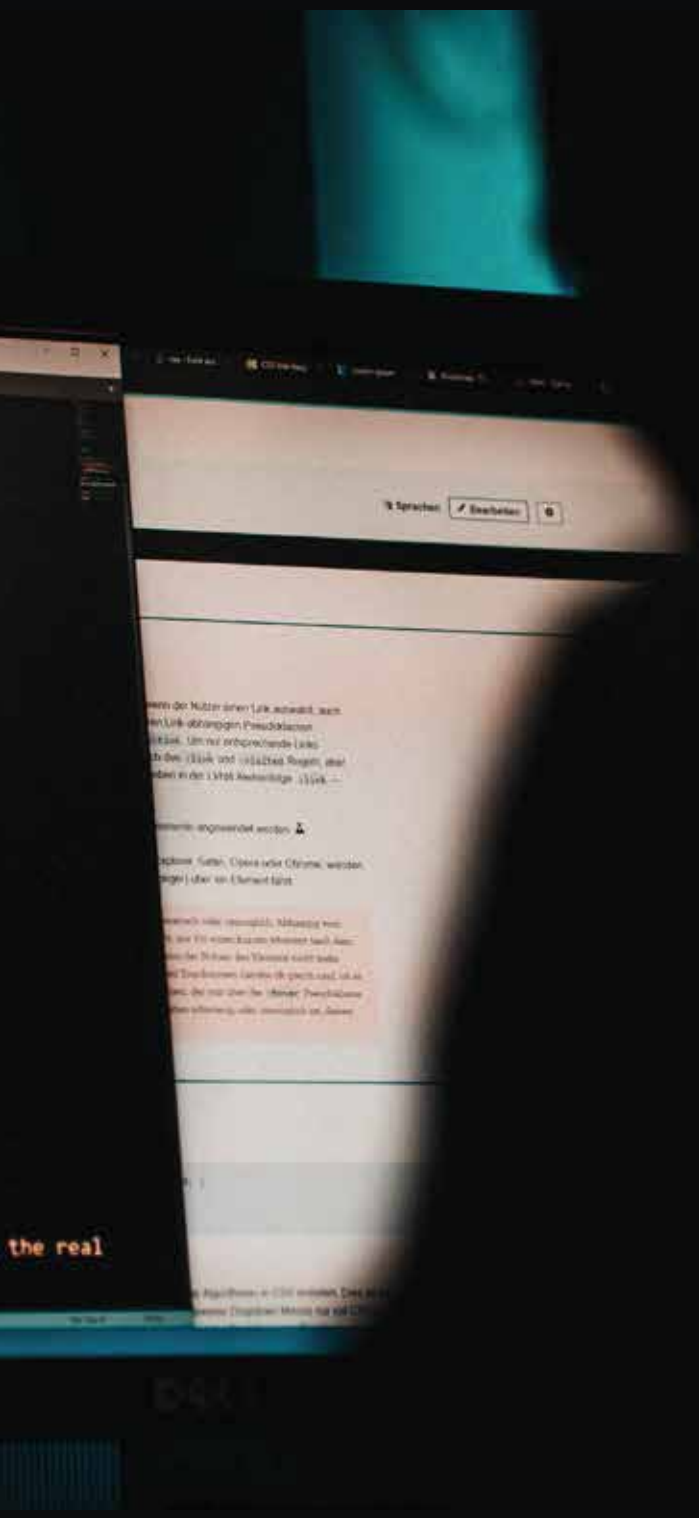
PRINCE2®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS

¿Hacia dónde se dirige la ciberseguridad en 2021?

Este 2021 que ahora comienza nos plantea escenarios bastante inciertos en materia de ciberseguridad.

Si es complejo plantearse hacia dónde va encaminada la ciberseguridad en una situación de normalidad, este planteamiento se dificulta debido a la situación actual en la que nos encontramos.

La *"implantación"* del teletrabajo de la forma en la que lo hemos hecho augura que el teletrabajo va a ser uno de los objetivos principales de los ciberdelincuentes durante este año 2021.
Conocido es por todos los lectores que los malos no descansan y han centrado gran parte de sus objetivos en los usuarios, que como hemos dicho en más de una ocasión, siguen siendo el eslabón más débil dentro de la empresa. El paso de trabajador a teletrabajador como hemos visto durante la segunda mitad de 2020 ha supuesto para muchas compañías, principalmente pequeña y mediana empresa, un quebradero de cabeza. Se han adaptado sistemas, muchos de estos nuevos teletrabajadores han tenido sus primeros contactos con VPN´s para acceder a los sistemas y aplicaciones corporativas y como solución a corto plazo es válida, pero no es la solución más acertada a medio/largo plazo.



Efectivamente, las VPN también son un vector de ataque que se está explotando de forma constante junto con la posibilidad que ofrecen algunas empresas del uso de los dispositivos del trabajador (Bring Your Own Device), ya que éstos carecen en la mayor parte de los casos de las medidas de seguridad apropiadas.

Muchas empresas han bajado su inversión en protegerse de ciberataques, se estima que en 2020 se ha reducido la inversión en torno a un 10%, lo que hace que las arquitecturas de seguridad pierdan parte de su efectividad y esto puede llevar a que las empresas sufran brechas de seguridad importantes.

No todo son malas noticias, ya que se buscan soluciones de seguridad como las denominadas redes de confianza cero, que se basan en que ningún usuario tiene acceso a ellas sin pasar por estrictas verificaciones de seguridad, tanto de personas como de dispositivos. En este tipo de redes la premisa es no confiar en nadie, ni de dentro ni de fuera de la organización. 2021 podría ser el principio de la generalización del uso de este tipo de redes.

Los datos sanitarios y los hospitales siguen y seguirán siendo, por desgracia, objetivos de los ciberdelincuentes. Muchas organizaciones o empresas sanitarias no disponen de niveles de seguridad apropiados y esto ha hecho que sean numerosas las brechas de seguridad que han dejado al descubierto información médica que debería de haber sido protegida.

CONTINÚA EN PRÓXIMA PÁGINA

Otro de los objetivos sobre los que pondrán sus ojos los delincuentes seguirá siendo el sector financiero. Ya lo fue durante el año que ha terminado y lo va a seguir siendo durante 2021.
Los datos financieros son otro de los platos favoritos de los ciberdelincuentes, un planteamiento proactivo de la seguridad respecto a la protección de datos es la línea por la que este tipo de compañías aboga.

La transformación digital que hemos vivido durante 2020 no será algo pasajero. El teletrabajo ha llegado para quedarse, hemos "*normalizado*" el uso de internet para hacer cosas que antes hacíamos fuera de la red, sobre todo las compras por internet.
El usuario doméstico será otro de los objeti vos para este año que empieza, el número de usuarios de internet aumenta y esto permite a los ciberdelincuentes realizar ataques con una mayor facilidad. Los ataques de ***vishing*** sobre los que hablábamos en nuestro anterior número van a ser otro punto de ataque para la obtención sobre todo de credenciales de acceso a redes corporativas.
La concienciación jugará un papel muy importante dentro de la seguridad durante este año 2021.

Y justamente eso es lo que quiero desearos a todos, un feliz, concienciado y seguro 2021.

fórmate!

https://businessandcompany.com/msp

Managing Successful Programmes MSP®

Curso de Gestión de Programas de Proyectos MSP® Fundamentos

MSP®

ACCREDITED TRAINING ORGANIZATION

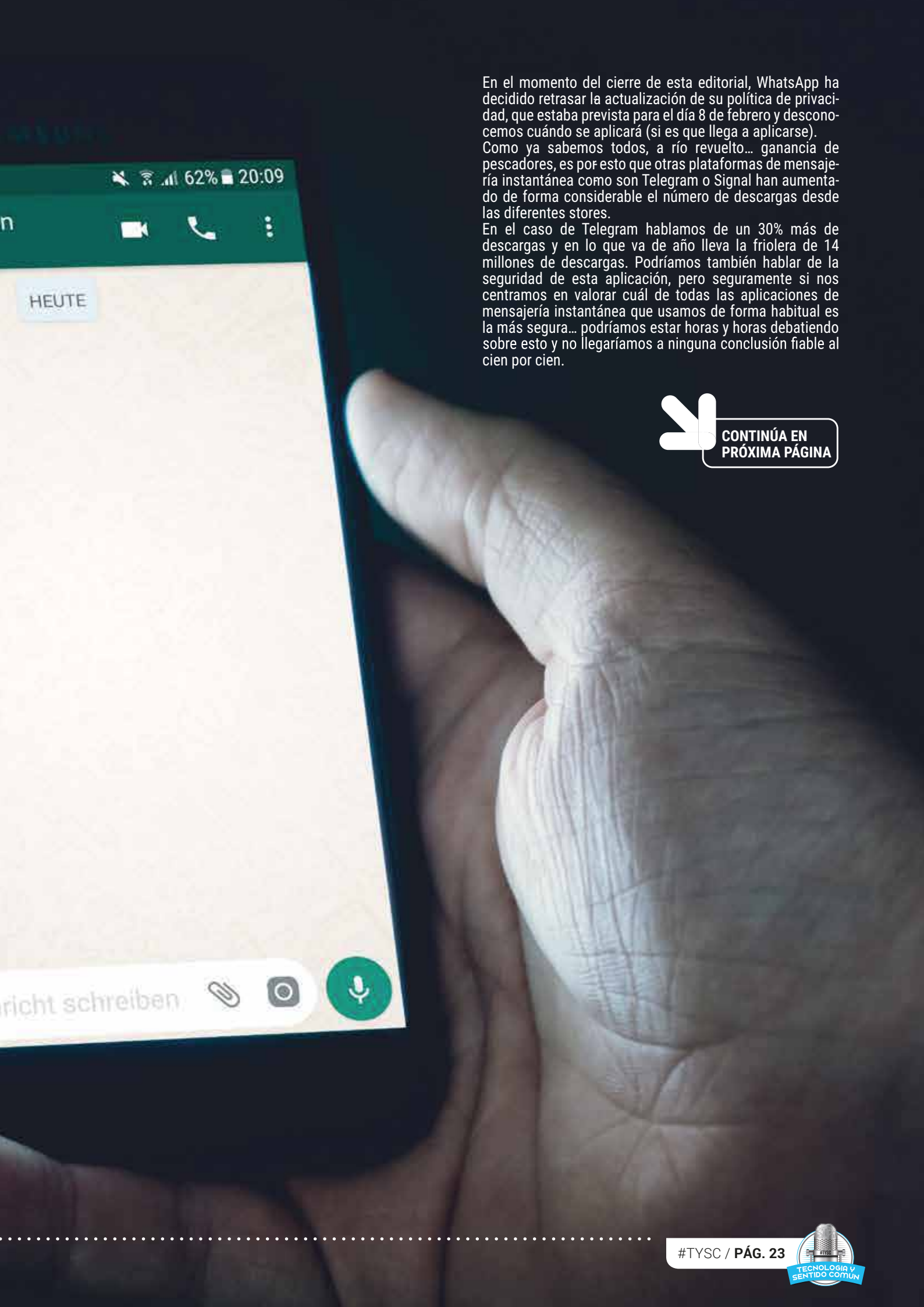
PeopleCert ON BEHALF OF AXELOS

Business&Co.®

Business, Technology & Best Practices, S.L.

¡¡Alarma!! Nueva política de privacidad en WhatsApp

El año comienza movido para WhatsApp. A principios del mes de enero, el servicio de mensajería WhatsApp comenzó a mostrar un aviso a sus usuarios informándoles que debían de aceptar las nuevas condiciones de privacidad o bien dejar de usar el servicio.
Dichas condiciones están relacionadas con el número de datos que WhatsApp comparte con Facebook y afectan a usuarios de la aplicación de fuera del territorio de la Unión Europea, es por esto, que dicho aviso no debería de haber aparecido a los usuarios europeos ya que estos cambios no afectarían a los mismos.
Según indica la propia compañía: '*No hay cambios en las prácticas de intercambio de datos de WhatsApp en la región europea (incluido el Reino Unido) que surjan de los Términos de servicio y la Política de privacidad actualizados. Para aclarar cualquier duda, sigue siendo cierto que WhatsApp no comparte datos de usuario de la región europea con Facebook con el fin de que Facebook utilice estos datos para mejorar sus productos o anuncios*'.
Teóricamente, y repito, en teoría, bajo la cobertura que otorga el GDPR no aplicaría a usuarios de la Unión Europea. ¿Puede que nos encontremos ante una maniobra de WhatsApp para '*colar un gol*' a los usuarios europeos? Por el momento desconocemos este aspecto.
Hemos podido comprobar como la Directora de Políticas de WhatsApp, Niamh Sweeney, utilizaba su perfil en Twitter (@NiamhSweeneyNYC) para desmentir que esta actualización de los Términos de Uso y la Política de privacidad de WhatsApp vaya a suponer cambios en Europa.



En el momento del cierre de esta editorial, WhatsApp ha decidido retrasar la actualización de su política de privacidad, que estaba prevista para el día 8 de febrero y desconocemos cuándo se aplicará (si es que llega a aplicarse).
Como ya sabemos todos, a río revuelto… ganancia de pescadores, es por esto que otras plataformas de mensajería instantánea como son Telegram o Signal han aumentado de forma considerable el número de descargas desde las diferentes stores.
En el caso de Telegram hablamos de un 30% más de descargas y en lo que va de año lleva la friolera de 14 millones de descargas. Podríamos también hablar de la seguridad de esta aplicación, pero seguramente si nos centramos en valorar cuál de todas las aplicaciones de mensajería instantánea que usamos de forma habitual es la más segura… podríamos estar horas y horas debatiendo sobre esto y no llegaríamos a ninguna conclusión fiable al cien por cien.

CONTINÚA EN PRÓXIMA PÁGINA

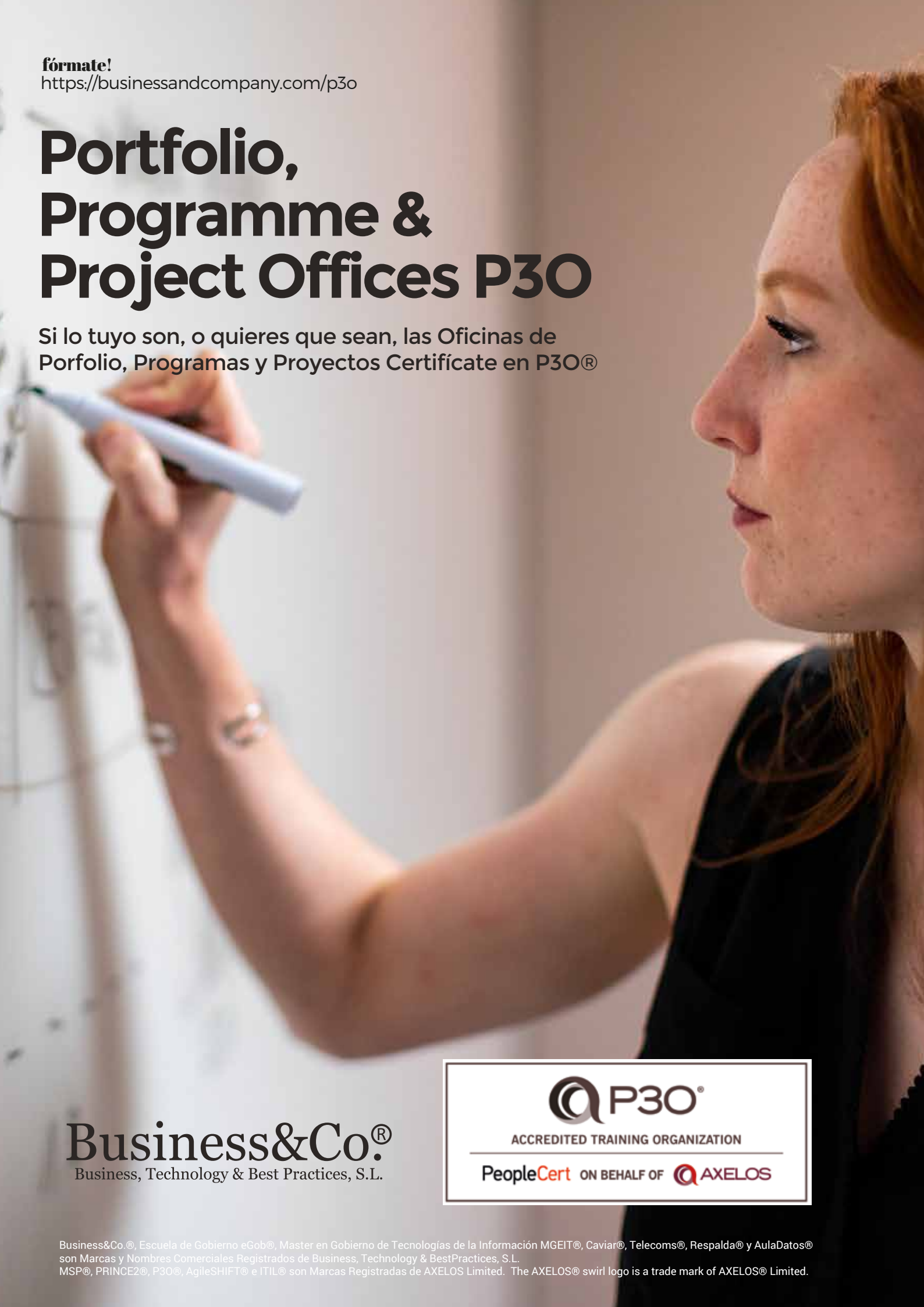
Por otro lado, nos encontramos con Signal, la gran beneficiada al comienzo de este año. Personajes públicos de la talla de Ellon Musk con un rotundo "***Usa Signal***" o Edward Snowden alegando como razón para su uso que "***la uso cada día y no está muerto todavía***" han hecho campaña a favor del uso de la misma durante este mes de enero y han catapultado esta aplicación que tenía un uso menos extendido entre usuarios domésticos. Ha llegado incluso a provocar que los servidores de Signal experimenten problemas debido a la saturación de los mismos, pasando de unas 25.000 descargas al día a más de 2 millones y llegando a ser la App número uno en numerosos países además de encontrarse en el top 10 de la mayoría de los restantes.

La privacidad empieza a ser importante para muchos de los usuarios, y se empieza a tener en cuenta por parte de los mismos. ¿Qué más veremos a lo largo de este año? No lo sabemos, nos encontramos ante un futuro bastante incierto. Valorar los pros y contras de cada una de las aplicaciones menciona das es difícil hasta para los expertos, y este comienzo de 2021 se presenta movido.
Elegir bien es complicado, valorar y conocer lo que hacen las empresas con nuestros datos personales es fundamental. Veremos qué pasa.

fórmate!
https://businessandcompany.com/p3o

Portfolio, Programme & Project Offices P3O

Si lo tuyo son, o quieres que sean, las Oficinas de Porfolio, Programas y Proyectos Certifícate en P3O®



Business&Co.®
Business, Technology & Best Practices, S.L.

P3O®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS

COMB, 3,2 Billones de contraseñas filtradas

Estimados lectores, si enero comenzó "*movidito*" por los cambios en la política de WhatsApp, febrero no lo va a ser menos. Este mes de febrero hemos visto la que hasta la fecha es la mayor filtración de usuarios y contraseñas, 3,2 billones.

Pero hablemos de números. Allá por el año 2017 se filtraron 1.400 millones de credenciales. El número de esta nueva filtración está en torno a 3.200 millones. Si la población de la tierra es de aproximadamente 7.500 millones de personas, hablaríamos de en torno al 40% de la población mundial (si cada registro fuera de una única persona).

COMB (Compilation Of Many Breaches), es un recopilatorio de las últimas filtraciones y ataques que se han producido en la red y que han dejado comprometidos a un elevado número de usuarios.

Ésta última compilación, que se filtró en un conocido foro a primeros del mes de febrero, contiene credenciales de "*leaks*" tan conocidos como el que tuvo Netflix, Minecraft, Badoo, LinkedIn, o incluso el archiconocido de Adobe allá por 2013.

El principal problema con el que nos encontramos es que hoy en día las filtraciones no pueden pararse. Pensamos que no utilizando determinados servicios podemos estar protegidos, pero nada más lejos que eso. Todos los lectores conocemos como muchas compañías, en base al uso de determinados servicios, venden datos a otras empresas de las que el usuario final no sabe absolutamente nada.

El valor de los datos, tanto en el mercado negro como a nivel corporativo, es muy elevado, y como todo en esta vida, cuanto más azúcar más dulce.
En el nuevo COMB nos encontramos algo más de 200 millones de cuentas de Gmail y en torno a 450 millones de cuentas de Yahoo. Esto puede llevar a preguntarnos ¿Ha existido alguna fuga de datos en Gmail? Hasta donde nosotros sabemos no, no ha existido brecha alguna, pero hemos de tener en cuenta que estas direcciones de correo se usan como acceso a otros servicios que tal vez sí que hayan tenido esa brecha.

CONTINÚA EN PRÓXIMA PÁGINA

¿Por qué son importantes los daños que este "*leak*" puede ocasionar? La gestión que como usuarios de internet hacemos de nuestras contraseñas deja bastante que desear y es habitual que muchos usuarios de internet utilicen la misma contraseña para acceder a diferentes sitios.
Protegernos a nivel de usuario de este tipo de filtraciones es más fácil de lo que parece. El cambio regular de contraseñas de acceso o el uso del doble factor de autenticación (al alcance de todos) mitigan enormemente los daños que una filtración de este tamaño puede ocasionar.

A nivel empresarial es muy importante que las credenciales corporativas vayan acompañadas de un segundo factor de autenticación o de un certificado en caso de credenciales de conexiones remotas.

¿Será ésta la última filtración que veremos? Probablemente no, lo que no podemos decir es cuándo la veremos porque este tipo de filtraciones son como los terremotos, no se pueden predecir ni controlar.

OSINT, cuando la información es poder

Las redes sociales se han convertido en un reflejo de lo que hacemos a diario, de nuestros gustos, de nuestras preferencias e incluso de nuestros hábitos y costumbres.

OSINT (Open Source INTeligence) son unas siglas que están muy vinculadas a ciberseguridad y que empiezan a ser una parte importante en el proceso de preparación de un ataque por parte de ciberdelincuentes. OSINT no es más que inteligencia extraída de fuentes abiertas con cualquier tipo de objetivo, tanto personal como empresarial. Si en algún momento de tu vida has sido capaz de extraer una conclusión sobre una persona o compañía en base a un tweet o a una fotografía publicada en Facebook o Instagram has empleado técnicas OSINT sin saberlo.

Esta técnica se basa en la obtención de cualquier tipo de información que se puede encontrar en internet sobre una persona o compañía concreta. Dicha información nos puede aportar tanto localizaciones, como hábitos, o información relevante sobre un presunto objetivo.

CONTINÚA EN PRÓXIMA PÁGINA

Analizar hasta el más mínimo detalle de una imagen, es una de las técnicas más comunes que existen a la hora de realizar una investigación OSINT, pero no es sólo la única. Un buen ejemplo puede ser la cantidad de datos indexados en buscadores como Google o Bing y aunque estas búsquedas se basan en algoritmos ya depurados que nos dan con facilidad los resultados que buscamos, ambos cuentan con una serie de búsquedas avanzadas que nos permiten afinar las mismas para obtener bastante más información del objetivo.

Nos podemos encontrar también con buscadores más específicos, como Shodan, buscador de equipos conectados a internet, ya conocido por la inmensa mayoría de los lectores, del que se pude obtener una gran cantidad de información.

Otra de las herramientas más utilizadas en la práctica de OSINT es Maltego, con esta herramienta podemos comprobar la exposición que empresas o personas tienen en internet, haciendo un barrido para de esta forma obtener una gran cantidad de información potencialmente interesante.

Dicha información se procesará y analizará a posteriori para obtener una serie de conclusiones. Es aquí donde entran en juego las distintas técnicas y herramientas para conseguirlo. Dependiendo de estas últimas, la inteligencia de código abierto puede ser activa, pasiva o en un punto intermedio entre ambas.

La diferencia entre ambas es que las herramientas que trabajan de forma pasiva no tienen como objetivo el almacenamiento de información sino ir filtrando poco a poco hasta llegar al punto deseado.

Dominios, correos electrónicos, nombres de usuarios, metadatos, geolocalización, números de teléfono, etc, van a proporcionar a los ciberdelincuentes la posibilidad de afinar muchísimo sus ataques.

Hemos de decir que este tipo de herramientas no son únicamente utilizadas por ciberdelincuentes. Fuerzas y Cuerpos de Seguridad del estado hacen uso de las mismas durante el desarrollo de sus investigaciones.

Desde Tecnología y Sentido Común hacemos especial énfasis en cuidar nuestra identidad digital para de esta forma dificultar en la medida de lo posible los ataques dirigidos (o no) que se puedan realizar contra personas/empresas.

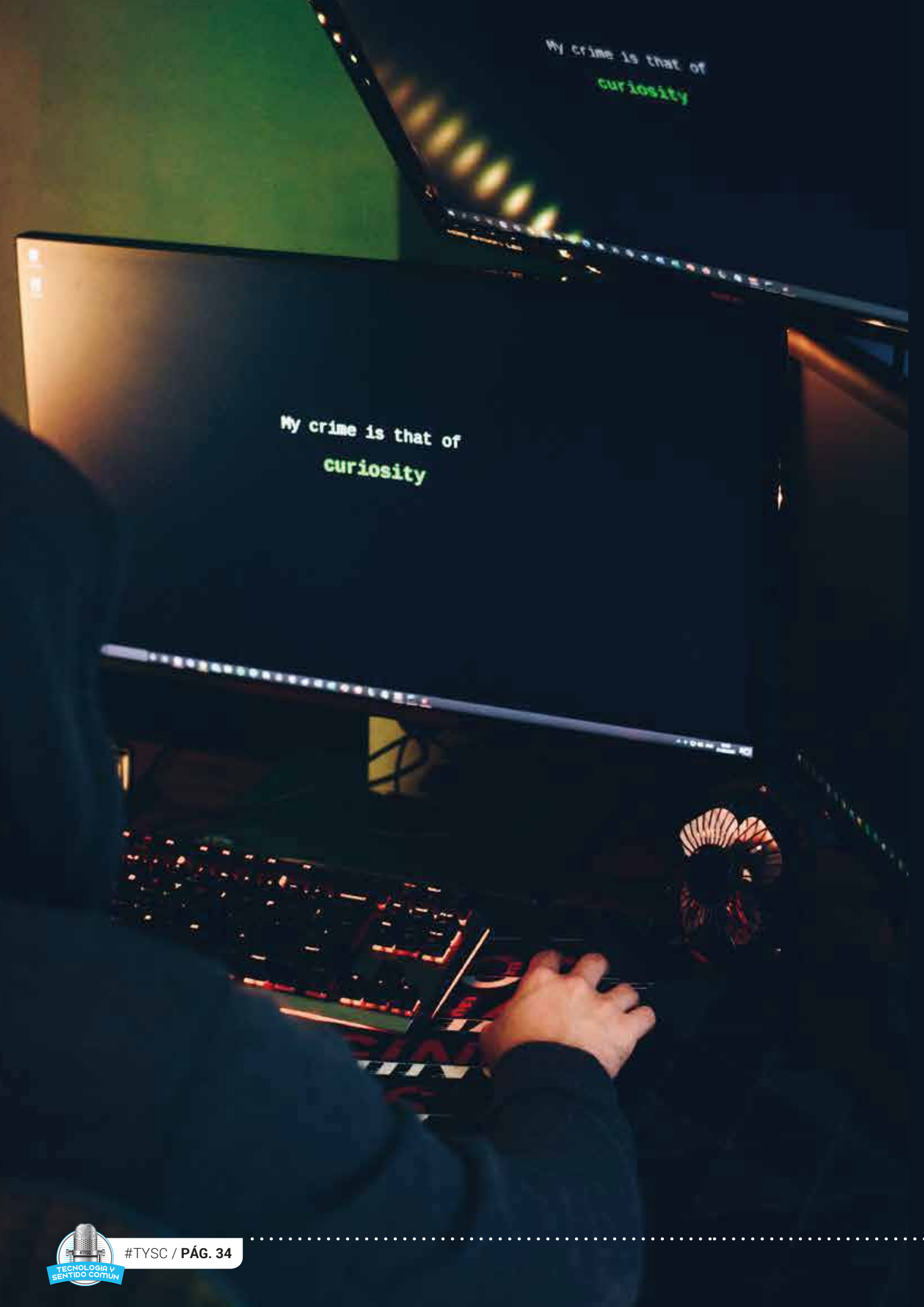
fórmate!
https://businessandcompany.com/cobit

Tu vida puede depender de la tecnología

COBIT® 2019 Marco de Gobierno y Gestión de la Tecnología

La Implementación de un Marco de Gobierno y Gestión de Tecnologías de la Información permite conocer la salud global de los Sistemas de Información de los que depende los procesos habituales de una organización, sin un adecuado Marco de Gobierno y Gestión se podrá trabajar la seguridad, privacidad y otros aspectos de manera disociada tampoco se podrá garantizar que se estén teniendo en cuenta todos los factores necesarios para una adecuada operación. COBIT® aporta confianza.

Business&Co.®
Business, Technology & Best Practices, S.L.


My crime is that of
curiosity
My crime is that of
curiosity

Mayo, mes del ciberdelicuente

En números anteriores hemos hablado de fugas y/o exfiltraciones de datos que se han ido produciendo durante los últimos meses. Allá por el mes de marzo nos hacíamos eco de la madre de las filtraciones, COMB, con 3.2 billones de contraseñas filtradas.

La última de estas filtraciones la hemos visto durante el pasado mes de abril, y esta vez, aunque con un número menor de datos, es bastante más jugosa para los ciberdelincuentes, ya que se trata de Facebook.

Más de 553 millones de usuarios, repartidos por 106 países de todo el mundo han visto comprometida la integridad de sus datos al ver como se hacían públicos datos tan importantes como el número de teléfono. Este *leak*, ha supuesto que, a nivel de España, 11 millones de usuarios han visto expuesta información tan notable como puede ser su número de teléfono.
¿Ha sufrido Facebook una brecha de seguridad? Hay opiniones de todo tipo, y al tratarse este artículo de un artículo de opinión voy a dar mi punto de vista (totalmente personal y no vinculante). Personalmente, creo que sí, que ha existido algún tipo de brecha de seguridad que ha permitido que estos datos sean publicados. ¿Cómo lo han hecho? A día de hoy el hermetismo es absoluto, "*nadie sabe nada*".

Otra de las opciones que se barajan es la obtención de dicha información mediante herramientas de extracción de datos (*Web scrapping*), una técnica que consiste en el "escaneo" de perfiles y sobre la que Facebook en concreto, tiene herramientas más que aceptables para protegerse.

Como podéis ver, estimados lectores, hay opiniones de todo tipo. Pero ¿de qué forma puede afectar esto a las personas que se han visto afectadas por esta exfiltración de datos?
Estos datos en manos de un ciberatacante son oro puro, en nuestro número del mes de diciembre hablábamos de *phishing, vishing y smishing*. Es para este último para el que un ciberdelincuente puede utilizar estos leaks. Los ataques dirigidos pueden alcanzar una precisión muy elevada al poseer este tipo de información.

Es muy posible que durante los meses que dure la campaña de la renta, en España observemos como los incidentes relacionados con *smishing* aumente de forma considerable. Pero no podemos pensar que esto afectará únicamente a los usuarios cuyos datos han quedado expuestos. A nivel empresarial toda esta información hace más vulnerable a las empresas ante los anteriormente mencionados ataques dirigidos.

CONTINÚA EN PRÓXIMA PÁGINA

Los equipos de seguridad, los de concienciación, y sobre todo el sentido común que siempre os proponemos desde nuestra revista van a jugar un papel muy importante durante este mes de mayo. Si recibís algún tipo de mensaje que os resulte poco habitual, o un tanto extraño, os aconsejo que consultéis con el remitente ante cualquier duda.

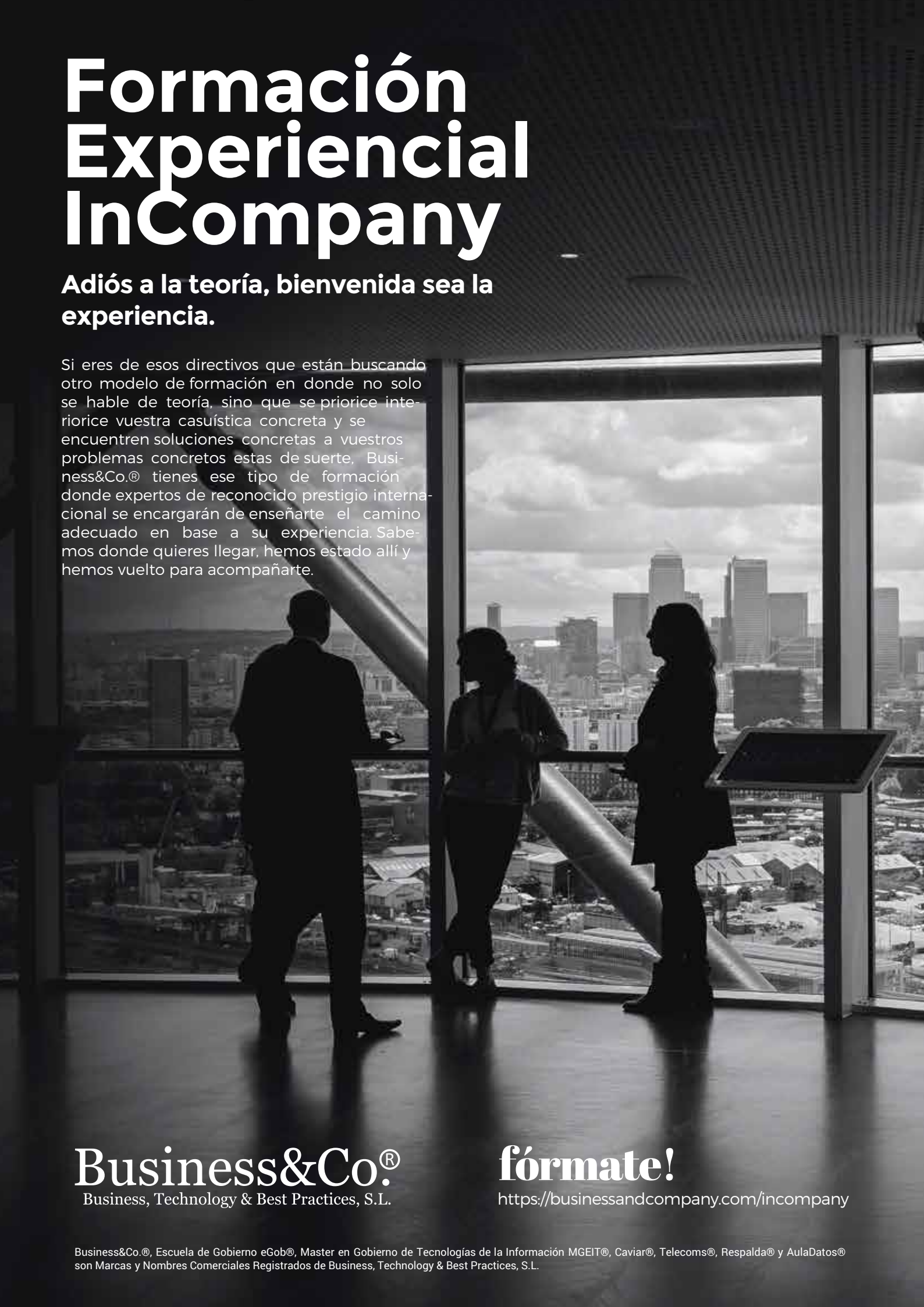
Si ese mensaje va acompañado de cualquier tipo de enlace, como os hemos indicado en ocasiones anteriores, no clickéis en el enlace. Este tipo de ataques suelen ir acompañados de malware mediante el cual un atacante puede obtener el control total del dispositivo con todo lo que ello implica.

Dicho esto, me queda únicamente desearos un feliz y seguro mes de mayo.

Formación Experiencial InCompany

Adiós a la teoría, bienvenida sea la experiencia.

Si eres de esos directivos que están buscando otro modelo de formación en donde no solo se hable de teoría, sino que se priorice interiorice vuestra casuística concreta y se encuentren soluciones concretas a vuestros problemas concretos estas de suerte, Business&Co.® tienes ese tipo de formación donde expertos de reconocido prestigio internacional se encargarán de enseñarte el camino adecuado en base a su experiencia. Sabemos donde quieres llegar, hemos estado allí y hemos vuelto para acompañarte.



Business&Co.®
Business, Technology & Best Practices, S.L.

fórmate!
https://businessandcompany.com/incompany

Ciberseguridad, ¿Inversión o gasto?

Ésta es una de las preguntas que más veces hemos podido leer o escuchar dentro del entorno empresarial. En la mayoría de los casos, cuando el CISO dice: *"Tenemos que aumentar la inversión en ciberseguridad"* el CEO piensa: *"Vamos a ver cuánto me cuesta esta vez lo que me piden"*.

La ciberseguridad se sigue viendo como un gasto y no como una inversión. Una encuesta realizada por la consultora Trend Micro, revela que hay un elevado nivel de concienciación sobre la seguridad. Un 64% de los encuestados afirman que, desde el inicio del confinamiento, y con la proliferación del teletrabajo, tienen más en cuenta este aspecto, aunque muchos de ellos reconocen no seguir al pie de la letra las políticas establecidas por sus departamentos de IT.

Las empresas han de elevar la inversión en ciberseguridad. La transformación digital *"sobrevenida"* de este último año ha hecho que el riesgo ante el cibercrimen aumente y obliga a las compañías a aumentar sus presupuestos en seguridad aún viendo disminuir los mismos en el departamento de IT.

En la actualidad las empresas demandan más inversión en ciberseguridad ante la multitud de amenazas crecientes. Tal vez estemos en un escenario donde la ciberseguridad jamás había sido tan visible ni la sociedad ha sido tan consciente de la dependencia existente hasta este momento.

El objetivo es claro, hay que aumentar la confianza de los usuarios y clientes y hemos de tener muy presente que sin confianza no hay economía. Un elevado número de los usuarios que prueban servicios digitales se acaban fidelizando y los mantienen. Esto conlleva dar un paso de gigante en una digitalización de la sociedad y de la economía.

CONTINÚA EN PRÓXIMA PÁGINA

El **Programa Europa Digital** pretende estimular la transformación digital de las empresas, ayudando a la financiación de algunas de sus áreas fundamentales. Esta iniciativa potenciará, entre otros aspectos, la inteligencia artificial y la supercomputación… Además de fomentar la **inversión en ciberseguridad**. Dicho programa tiene como objetivo estimular la transformación digital de las empresas, ofreciéndoles la financiación necesaria para que puedan adoptar las tecnologías más innovadoras en sus principales áreas de funcionamiento y ocupando la ciberseguridad el tercer puesto en presupuesto, con un presupuesto en torno a los 1.650M de euros.

Los retos a los que nos encontramos en el ámbito de la ciberseguridad incluyen desde la lucha contra la ciberdelincuencia al refuerzo de la ciberdefensa, la protección de las infraestructuras críticas y la mejora de la ciberresiliencia; entre otros aspectos importantes.

Desde el punto de vista de los departamentos financieros, el beneficio obtenido al realizar inversiones en seguridad es difícil de calcular. Normalmente es más fácil cuantificar el coste de un incidente de ciberseguridad en el caso de que se hubiera materializado. Este dato es el resultado del tratamiento o análisis de riesgos que toda organización debe de tener dentro de un modelo de Gobierno, Riesgo y Cumplimiento (GRC) para garantizar la gestión del riesgo integral y determinar en todo momento si las medidas o controles implantados son suficientes para hacer frente a riesgos corporatimos.

Es muy importante considerar la ciberseguridad como una **inversión,** ya que de ello va a depender el buen funcionamiento de la compañía. La seguridad es una inversión y no se debe considerar nunca un gasto "supérfluo".

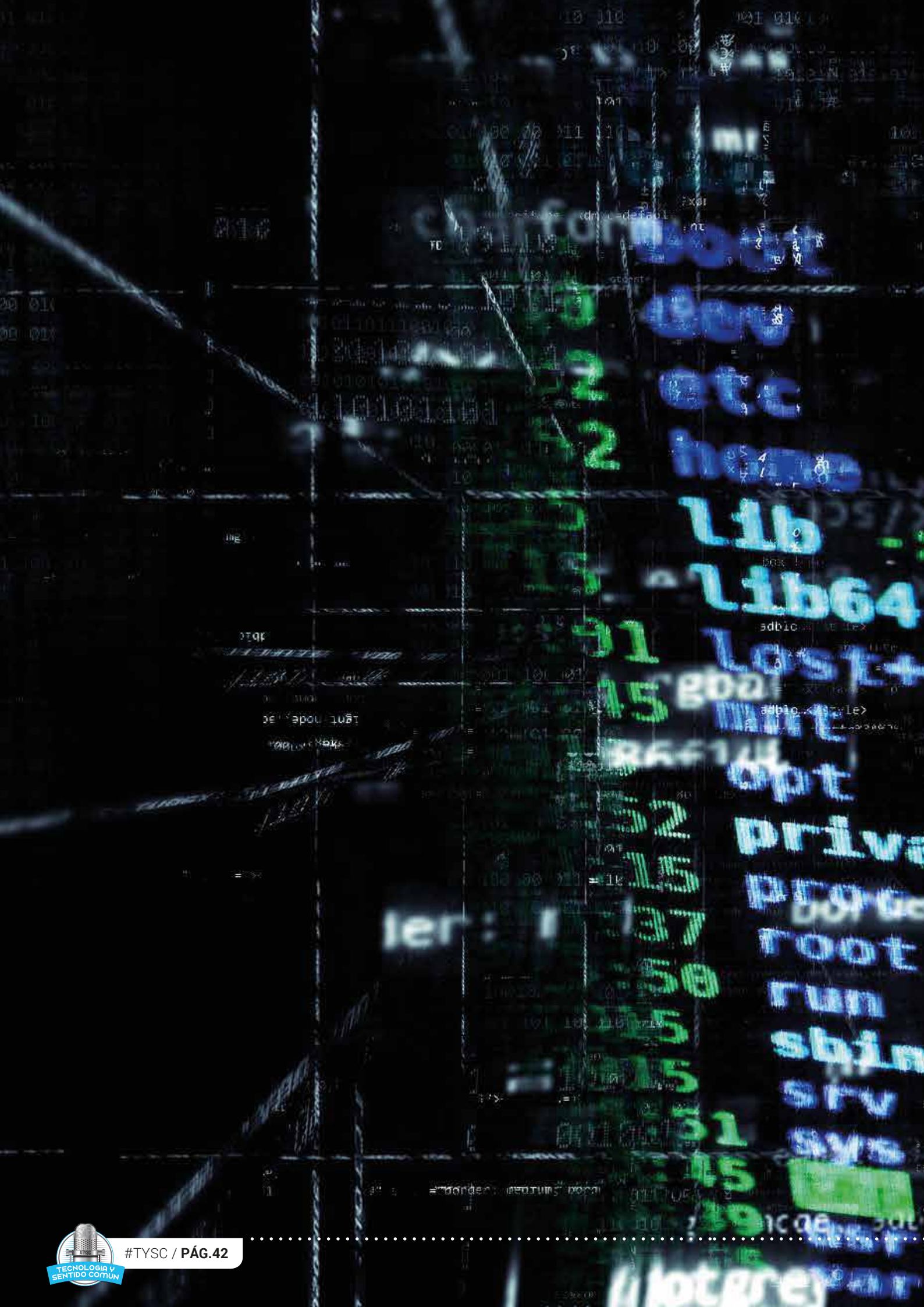
fórmate!
https://businessandcompany.com/itil

El Sistema de Valor del Servicio de ITIL®4

...o todavía andas pensando en el ciclo de vida del Servicio.

Business&Co.®
Business, Technology & Best Practices, S.L.

ITIL®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS


dev
etc
home
lib
lib64
lost+found
mnt
opt
priva
proc
root
run
sbin
srv
sys

We will rock you

Cuando escuchamos o leemos esta frase, es imposible no acordarse de la archiconocida canción del grupo inglés Queen, pero los que tenemos de alguna forma relación con la informática, vamos a recordarla desde este mes pasado de junio por ser hasta la fecha el mayor leak de contraseñas que jamás se ha publicado.

Cuando allá por el mes de marzo salió a la luz COMB (Compilation Of Many Breaches) nos quedamos sorprendidos por la cantidad ingente de información que se había filtrado. Cerrábamos nuestro artículo de "Tecnología y Sentido Común" con la pregunta de si sería esta la última filtración de este tamaño con la que nos encontraríamos, pues bien, ya tenemos respuesta, COMB no era la última. Con el inicio de la temporada estival aparece en escena RockYou2021, y si COMB nos hacía respirar de forma profunda, RockYou2021 nos hace temblar.

Un conocido sitio de la deepweb alojó durante varios días esta última compilación de contraseñas. ¿La cantidad? **Exactamente 8.459.060.239 contraseñas**, en un archivo brutal de un peso de 100Gb. Para hacernos una idea de la magnitud que esto representa, y como dato orientativo, hemos de decir que la base de datos de la conocida web Have I Been Pwned está formada por casi 11.400 millones de contraseñas.

Todas las contraseñas de esta nueva filtración aparecen en texto plano y están formadas por contraseñas de entre 6 y 20 caracteres donde han sido eliminados caracteres que no son ASCII y los espacios.

CONTINÚA EN PRÓXIMA PÁGINA

Pero volvamos a la relevancia de este archivo. A parte del tamaño que tiene, y si tenemos en cuenta que según Wikipedia el número de usuarios con acceso a internet es de unos 4665 millones, implica que podría haber al menos dos de tus contraseñas en este fichero.

El listado contiene únicamente las contraseñas, sin añadir el detalle de a qué servicio, página web, plataforma o dirección de correo electrónico se corresponden, pero a pesar de ello RockYou2021 constituye una herramienta muy útil para los ciberdelincuentes. Por ejemplo, se podría incluir esta base de datos y realizar un ataque denominado Spraying Password, que consiste en concentrarse en una única cuenta comprobando todas las contraseñas que contiene su diccionario, probando en primer lugar las más frecuentes.

Pero ¿Qué son los diccionarios de crackeo? son listas de contraseñas esperadas o, como dice el NIST, contraseñas de uso común o fáciles de adivinar. Estas listas se utilizan para revertir rápidamente contraseñas hash, para borrar texto o realizar ataques con el fin de adivinar una contraseña.

Adivinar la contraseña de alguien a partir de un conjunto de hashes descargado no es exactamente fácil; Pero puede hacerse. Esa es la razón por la que existen listas de contraseñas como RockYou2021. Estos volcados no sirven como una lista de contraseñas reales, sino más bien como una lista de posibles conjeturas para alimentar las herramientas que utilizan los ciberdelincuentes para intentar adivinar algunos de estos valores hash.

Hay quien asocia el hackeo de Colonial Pipeline con RockYou2021, la mayoría de las evidencias indican que no, pero es cierto que la contraseña utilizada para acceder a Colonial Pipeline se encuentra en la lista de RockYou2021. El problema es que no se trata de una lista única, sino de una complicación de varias listas.

En estas vacaciones, que espero estéis disfrutando lo máximo posible, al igual que os protegéis del "*solete*" con un buen protector, proteged también vuestras credenciales. No nos cansaremos de decirlo, cambiar la contraseña de forma periódica y utilizar el doble factor de autenticación (2FA) os puede evitar muchísimos quebraderos de cabeza.

¡Disfrutad del verano! ¡Nos leemos pronto!

#BestPractices #BetterProfessionals

Cursos oficiales de Certificación

septiembre

GOBIERNO I&T

COBIT® 2019 FUNDAMENTOS

PRIMERA SESIÓN:
Viernes 3 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 4 de Septiembre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 10 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
Sábado 11 de Septiembre de 2021 de 09:00 a 14:00 horas

GESTIÓN DE SERVICIOS

ITIL® 4 FUNDAMENTOS

PRIMERA SESIÓN:
Martes 7 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 9 de Septiembre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 14 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Jueves 16 de Septiembre de 2021 de 16:00 a 21:00 horas

GESTIÓN POR PROCESOS

BPM PROFESIONAL ISO/IEC 19510

PRIMERA SESIÓN:
Viernes 17 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 18 de Septiembre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 24 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Sábado 25 de Septiembre de 2021 de 09:00 a 14:00 horas

GESTIÓN DE SERVICIOS

ITIL® 4 STRATEGIST: DIRECT, PLAN & IMPROVE

PRIMERA SESIÓN:
Martes 21 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 23 de Septiembre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 28 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Jueves 30 de Septiembre de 2021 de 16:00 a 21:00 horas

octubre

GESTIÓN DE SERVICIOS

ITIL® 4 FUNDAMENTOS

PRIMERA SESIÓN:
Viernes 1 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 2 de Octubre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 8 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Sábado 9 de Octubre de 2021 de 09:00 a 14:00 horas

GOBIERNO I&T

COBIT® 2019 FUNDAMENTOS + ISO 38500 PROFESIONAL

PRIMERA SESIÓN:
Martes 5 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 7 de Octubre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 12 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
ISO/IEC 38500 a elegir por el Alumno.

GESTIÓN DE PROYECTOS

PRINCE2® FUNDAMENTOS

PRIMERA SESIÓN:
Viernes 15 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 16 de Octubre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 22 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
Sábado 23 de Octubre de 2021 de 09:00 a 14:00 horas

GESTIÓN OFICINAS DE PROYECTOS

P3O® FUNDAMENTOS

PRIMERA SESIÓN:
Martes 19 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 21 de Octubre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 26 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
Jueves 28 de Octubre de 2021 de 16:00 a 21:00 horas

Business&Co®
Business, Technology & Best Practices, S.L.

Más información en
https://javierperis.com/formacion-oficial/