ESPECIAL

“Futuro y seguridad”

DE Tecnología & Sentido Común

AGOSTO
2022

RANSOMWARE-4AS-A-SERVICE: 12
Otra vuelta de tuerca

16
La concienciación en ciberseguridad

20
EIDAS-2 y la identidad basada en Blockchain

QUÉ ES Y CÓMO PROTEGERSE DE LA 24
amenaza de la Ingeniería Social (I)

QUÉ ES Y CÓMO PROTEGERSE 28
de la amenaza de la Ingeniería Social (II)

32
QUÉ ES Y CÓMO PROTEGERSE DE LA AMENAZA DE LA INGENIERÍA SOCIAL (Y III)

OSINT, o qué puede saber cualquiera sobre nosotros 36

40
El Plan Nacional de Ciberseguridad

44
Consejos de Ciberseguridad (I)

48
Consejos de Ciberseguridad (y II)

safecreative
2 010025 512318
INFO ABOUT RIGHTS

ESPECIAL "Futuro y seguridad" DE Tecnología & Sentido Común

EQUIPO TYSC
Javier Peris - El Gobernauta
Manuel D. Serrat - Futuro y Seguridad
Fernando Roca - Talento y Liderazgo
Alberto Rodríguez - Hack & News
Juan Carlos Muria - Salud en la Nube
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Catalina Valencia - Ecosistema Emprendedor
Marcos Navarro - Ai Robot
Víctor Almonacid - La Nueva Administración
Shirley Aristondo - América Próxima
Madelaine Castro - Por Procesos
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

safecreative
2 010025 512318
INFO ABOUT RIGHTS

(Business&Co.®) Business, Technology & Best Practices, S.L. en ningún caso y bajo ningún supuesto se hace responsable de las opiniones aquí expresadas por sus colaboradores o entrevistados.

Business&Co.®, Escuela de Gobierno eGob®, Master en Gobierno de Tecnologías de la Información MGEIT®, Caviar®, Telecoms®, Respalda® y AulaDatos® son Marcas y Nombres Comerciales Registrados de Business, Technology & Best Practices, S.L. MSP®, PRINCE2®, P3O®, AgileSHIFT® e ITIL® son Marcas Registradas de AXELOS Limited. The AXELOS® swirl logo is a trade mark of AXELOS® Limited. El Resto de marcas y Logotipos son de sus respectivos propietarios.COBIT® es una Marca Registrada de ISACA.

MANUEL SERRAT OLMOS

Doctor en Informática por la Universidad Politécnica de Valencia, Master en Dirección de TIC por la UPM, dispone de varias certificaciones internacionales en Operación, Gestión y Gobierno de TI ITIL, PRINCE2 y COBIT5, es escritor técnico, ha sido profesor asociado en la UPV y actualmente dirige el departamento de TI en una organización pública, y Responsable del Comité de la Comunidad Valenciana de itSMF España.

LinkedIn:
https://www.linkedin.com/in/manuel-david-serrat-olmos/

Twitter:
https://twitter.com/mdserrat

©2020 Business&Co.® - Todos los Derechos Reservados.

27-28 SEPTIEMBRE | VIRTUAL | GRATUITO

DIGITALIZE AND AUTOMATE

UNO DE LOS MAYORES EVENTOS SOBRE LA DIGITALIZACIÓN DE EMPRESAS EN EUROPA

5000 PARTICIPANTES

25 PONENTES, LÍDERES Y EXPERTOS DIGITALES

1 INVITADO SORPESA

2 DÍAS DE CONTENIDO EXCLUSIVO

INNOVACIONES TECNOLÓGICAS

CASOS DE ÉXITO

Participa en Digitalize and Automate 2022, uno de los mayores y más emocionantes eventos de **#ITSM, #IAM** y **#ESM** de Europa.

Celebramos que Efecte ya está disponible en España, y durante el evento lanzaremos una **oferta en exclusiva para las empresas españolas.** ¡Te esperamos!

efecte

REGÍSTRATE

www.efecte.es/digitalize-and-automate-2022

Premios recibidos

Premio Medio de Comunicación 2018 de la Asociación Profesional Española de Privacidad

La Junta Directiva de la Asociación Profesional Española de Privacidad durante su VI Congreso Nacional de Privacidad APEP celebrado en Madrid otorga el Premio Medio de Comunicación 2018 a Tecnología y Sentido Común #TYSC

Premio 2016 a la Difusión de los Valores de la Gestión y Gobierno TI

El Foro de Profesionales de la Gestión del Servicio en España itSMF otorga a «Tecnología y Sentido Común» el Galardón 2016 a la Difusión de los Valores de la Gestión y Gobierno de Tecnologías de la Información.

Tecnología y Sentido Común "Premio Sapiens" Medio de Comunicación 2022"

El Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana entregó el Premio Sapiens Medio de Comunicación 2022 a nuestra Revista "Tecnología y Sentido Común #TYC". El Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana COIICV alabó tanto la gran labor de difusión que viene realización Tecnología y Sentido Común desde hace siete temporadas como su capacidad de adaptación y resiliencia adaptándose a nuevos formatos con los que continuar en su labor de evangelización en Buenas Prácticas al conjunto de los profesionales a pesar de la alerta sanitaria con nuevos formatos que partiendo de un programa de Radio y Podcast han permitido seguir llevando su mensajes a través de la Revista Mensual, o el informativo televisivo "El Semanal" de Tecnología y Sentido Común.

COLEGIO OFICIAL DE INGENIERÍA INFORMÁTICA DE LA COMUNITAT VALENCIANA

Pasos firmes
Comprueba cómo los estándares ayudan a tu empresa
www.pasosfirmes.es
UNE
Asociación Española de Normalización
une@une.org - www.une.org -
Organismo de normalización español en
ISO
IEC
CEN
CENELEC
ETSI
COPANT

ESPECIAL AGOSTO 2022

índice

DE CONTENIDOS

https://tecnologiaysentidocomun.com

EIDAS-2 y la identidad basada en Blockchain

Qué es y cómo protegerse de la amenaza de la Ingeniería Social (II)

OSINT, o qué puede saber cualquiera sobre nosotros

Consejos de Ciberseguridad (y II)

índice

Índice de Contenidos — 06

El talento en Ciberseguridad: escasez y retención — 08

Ransomware- 4as-a-service: Otra vuelta de tuerca — 12

La concienciación en ciberseguridad — 16

EIDAS-2 y la identidad basada en Blockchain — 20

Qué es y cómo protegerse de la amenaza de la Ingeniería Social (I) — 24

Qué es y cómo protegerse de la amenaza de la Ingeniería Social (II) — 28

Qué es y cómo protegerse de la amenaza de la Ingeniería Social (y III) — 32

OSINT, o qué puede saber cualquiera sobre nosotros — 36

El Plan Nacional de Ciberseguridad — 40

Consejos de Ciberseguridad (I) — 44

Consejos de Ciberseguridad (y II) — 48

#TYSC

El talento en Ciberseguridad: escasez y retención

Tras el asueto veraniego, iniciamos temporada de #TYSC con un tema algo polémico. Desde hace unos años, se escuchan, en ciertos medios, datos acerca de la escasez de perfiles de ciberseguridad en el mercado laboral, y del volumen de empleo que ese sector va a generar en los próximos años. Sin embargo, también hay voces que apuntan a que no faltan perfiles, sino que las compañías no quieren asumir los costes que incorporar uno de estos valiosos profesionales tendría en sus cuentas de resultados. Si la Ley de la Oferta y la Demanda hace que los salarios de ese personal tengan que crecer, es lógico que el mercado intente generar más talento en ese ámbito para aumentar la oferta.

El pasado mes de junio, desde el Centro de Seguridad TIC de la Comunidad Valenciana (CSIRT-CV), dependiente de la Conselleria d'Hisenda i Model Econòmic de la Generalitat Valenciana, se lanzó la campaña "Hazte analista de ciberseguridad"[1], en la cual, durante unas semanas, se publicaron mensajes en redes sociales alusivos a las posibilidades laborales que el ámbito de la ciberseguridad podían proporcionar a los futuros profesionales, citando los roles más demandados: analista de seguridad, de malware, de código fuente o forense, pentester, experto en ciberinteligencia y ciberfraude, etc.

¿De dónde proviene el interés de una Administración Pública en promocionar que los jóvenes valencianos o españoles se interesen en formarse en ciberseguridad como forma de labrarse un futuro profesional? Obviamente, una entidad como CSIRT-CV tiene en su plantilla profesionales del sector, y colabora con empresas punteras del mismo, por lo que probablemente conoce las dificultades que, según algunas fuentes, tienen las empresas en cubrir este tipo de puestos.

Esta dificultad alegada por el mercado tiene un refrendo en datos procedentes de diferentes estudios. En 2017, el Global Information Security Workforce Study (GISWS)[2] predecían que en 2022 la falta de profesionales de ciberseguridad a nivel mundial alcanzaría los 1,8 millones, y en el mismo estudio de 2019 vaticinaban ya que esa carencia alcanzaría los 4 millones. Otras fuentes[3] cifraban en 3,5 millones los puestos en ciberseguridad que no se iban a cubrir en 2021.

La cuestión que surge al leer este tipo de estudios es si realmente existe esa pretendida escasez de este tipo de profesionales. Porque si realmente existe, y es del volumen estimado, los portales y oficinas de empleo de los paises desarrollados deberían estar empapeladas con las ofertas de puestos de trabajo en ciberseguridad. Y no da la impresión de que lo estén, a tenor de las ofertas existentes en portales especializados[4] en reclutamiento de expertos en ciberseguridad a nivel internacional, ya que en el momento de escribir este artículo se localizaban 49 puestos ofertados. Recurriendo a portales de empleo en España, el portal líder ofertaba solamente 313 vacantes que, desde algún punto de vista, tienen que ver con la ciberseguridad.

CONTINÚA EN PRÓXIMA PÁGINA

Si extrapolamos este dato en función de la población española, la demanda de perfiles de ciberseguridad en 2021, teniendo en cuanta una duración media de 4 semanas de los anuncios de reclutamiento, sería aproximadamente de 1.212.043 puestos vacantes, lo cual coincidirán conmigo en que es una cota superior muy optimista, dado que muchos paises no tendrán ese nivel de demanda. Se puede concluir, por tanto, que la demanda de profesionales no alcanza ni de lejos lo previsto en los estudios antes citados. Entonces, ¿por qué se sigue repitiendo este mantra de la falta de profesionales en ciberseguridad?

Destacados miembros de la comunidad de ciberseguridad española, como Román Ramírez, fundador de RootedCon, tienen opiniones muy claras al respecto[5]: no falta talento, sino que falta que ese talento se pague como debe. Hay que ser conscientes de que el coste salarial de los expertos en ciberseguridad impacta en las cuentas de resultados de las empresas, y dificulta la venta de sus productos y servicios, al reducir su competitividad en precios. Sin embargo, no se aprecia el impacto positivo que este tipo de perfiles puede tener en las empresas que los incorporan, y los directivos se quejan de esos costes adicionales, que creen que minorarían si pudieran ofertar salarios más bajos porque hubiera mucha oferta de profesionales, pero no se dan cuenta de que están compitiendo por esos recursos en un mercado global, ya que los profesionales españoles pueden (y lo son) ser captados por empresas de cualquier punto del planeta.

Hay que tener en cuenta que, como en otros ámbitos, no es lo mismo trabajar en ciberseguridad que ser un experto en la materia, y a los expertos se les ha de pagar como a tales. Cuando se oyen quejas sobre la falta de personal en ciberseguridad, cabe recordar que según el SEPE el salario promedio en ciberseguridad en España son 23.700 euros brutos al año. Y lo que pretenden las empresas españolas, pagando esos salarios, es obtener perfiles expertos que en otros países están muchísimo mejor valorados económicamente y donde, además, desde siempre se les ha dado la posibilidad de teletrabajar, aspecto que en España sólo se ha abordado debido a la pandemia. Imaginense cobrando un salario del Reino Unido o EE.UU, pero residiendo en España. La solución a la falta de talento está al alcance de su mano: como dijo el Presidente Biden en junio a un grupo de empresarios que se quejaban de que no encontraban determinados perfiles, “paguenles más”.

Y cuando una empresa consigue captar una plantilla de profesionales equilibrada, profesional, bien considerada, tanto en salario contante y sonante como en salario emocional, y que saca sus proyectos adelante con un nivel de calidad excelente y ajustándose a los plazos previstos, ¿qué puede o debe hacer para retener ese talento? De eso, de la retención del talento, se ha escrito mucho y bien también en los últimos tiempos, pero me centraré en un aspecto diferencial de este sector.

Algunos estudios revelan que el 68% de los profesionales de la ciberseguridad opinan que una carrera profesional en ciberseguridad es increíblemente agotadora, y el 38% indican que la escasez de personal cualificado ha conducido tanto al agotamiento como al desgaste. En otras palabras, la escasez de perfiles en ciberseguridad puede convertirse en un círculo vicioso. Al no haber suficientes profesionales, las personas que se dedican a este trabajo son más propensos a quemarse, y cuando lo hacen y causan baja, la escasez se agrava, lo que lleva a un mayor agotamiento del resto.

Por tanto, es necesario que haya un mayor número de profesionales disponible para que el trabajo se dimensione adecuadamente y no suponga una fuente de riesgo psicológico para la salud de quienes lo ejercen. Pero al mismo tiempo, si no se quiere entrar en una espiral de volatilidad de la plantilla, hay que mantener una remuneración adecuada, y no sólo salarial, al trabajo realizado, evitando querer ganar competitividad por la vía de los bajos salarios. Quizá sería mejor que las compañías enfocasen el asunto planteándose qué impacto tendrían en sus cuentas de resultados, y **en su reputación**, determinados incidentes de ciberseguridad, y entonces tal vez los sueldos que les pidan sus candidatos a puestos de ciberseguridad en su empresa les parecerán baratos.

REFERENCIAS

[1] https://www.csirtcv.gva.es/nueva-campana-csirt-cv-hazte-analista-de-ciberseguridad/
[2] https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx
[3] https://www.itdigitalsecurity.es/actualidad/2020/03/35-millones-de-vacantes-en-ciberseguridad-no-se-cubriran-en-2021
[4] https://www.cybersecurityjobs.net/
[5] https://escudodigital.com/ciberseguridad/mesa-de-debate-antonio-fernandes-vigo-pasado-presente-y-futuro-de-la-ciberseguridad-sueldos-roman-ramirez/

MGEIT® MPPM®

eGob®

TSG4® Yellow Belt + Green Belt
Time Slot Governance
Gestión del Tiempo

COMIENZA POR
ORGANIZARTE

Si vas desbordado, te cuesta cumplir con las necesidades de negocio, no eres capaz de evidenciar el valor que aportas y no te da la vida para implantar Buenas Prácticas comienza por organizarte tú y organizar tu equipo con Time Slot Governance TSG4® Porque lo que no es Método es Improvisación

NIVELES DE CERTIFICACIÓN

TSG4® YELLOW BELT*
Forma y Certifica a Resposables y Miembros del Equipo en la Metodología de Gestión del Tiempo Time Slot Governance TSG4®

TSG4® ORANGE BELT*
Reconoce y Certifica a Miembros del Equipo que aplican la Metodología de Gestión del Tiempo Time Slot Governance TSG4®

TSG4® GREEN BELT*
Forma y Certifica a Responsables de los Equipos en la Metodología de Gestión del Tiempo Time Slot Governance TSG4®

TSG4® BROWN BELT*
Reconoce y Certifica a Responsables de Equipos que aplican la Metodología de Gestión del Tiempo Time Slot Governance TSG4®

TSG4® BLACK BELT*
Forma y Certifica a Implementadores de Buenas Prácticas con la Metodología de Gestión del Tiempo Time Slot Governance TSG4®

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones de 5 horas en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Cursos de Doble Certificación convalidables por asignaturas de los Masters MasterGEIT® y/o MasterPPM®.

CONVOCATORIAS 2022/23

- **TSG4® Yellow Belt + Green Belt (Martes y Jueves Tardes)**
  TSG4® Yellow Belt 15 de Septiembre de 2022 (Miércoles)
  TSG4® Green Belt 4, 6, 8 y 12 de Junio de 2023 (Martes y Jueves)
- **TSG4® Yellow Belt + Green Belt (Viernes Tardes y Sabados Mañana)**
  TSG4® Yellow Belt 1 de Octubre de 2022 (Sábado)
  TSG4® Green Belt 7, 8, 14 y 15 de Julio de 2023 (Viernes y Sábados)

eGob®

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es

Ransomware-as-a-service: Otra vuelta de tuerca

Son varios los artículos que hemos dedicado en números anteriores de Tecnología y Sentido Común al tema del ransomware, sin duda una de las peores amenazas para nuestro mundo cada vez más digitalizado. En alguno de esos artículos nos hemos referido a este fenómeno como un negocio lucrativo, y ahora ya se dispone de abundante información de cómo funciona y del nivel de industrialización que ha conseguido desarrollar.

En mi artículo del mes de octubre de 2020 de esta publicación[1] ya citaba el *ramsomware* como un lucrativo negocio, y uno de los principales fenómenos actuales del panorama de las amenazas a la ciberseguridad en las redes, si no el peor. Al principio, fue un mecanismo oportunista, basado en campañas masivas y poco sofisticadas, y que buscaban muchas infecciones, a cuyas víctimas se les exigía una cantidad relativamente baja de rescate. Estos ataques aprovechaban la sonrojante falta de seguridad de muchos sistemas de información por todo el planeta, sobretodo, equipos domésticos y de PYMEs, como ya analizamos en su día.

Sin embargo, esta industria otrora artesanal, ha evolucionado rápidamente en varios aspectos:

1. **ALCANCE:** aunque siguen habiendo campañas de ransomware 'para todos los públicos', cada vez más los ataques son dirigidos a entidades concretas, a las que creen que se les va a poder exigir un sustancioso rescate. Los ciberdelincuentes han atacado grandes empresas, hospitales, universidades y hasta ministerios, mediante técnicas muy sofisticadas y elaboradas ad hoc para la entidad víctima.

2. **OSADÍA:** en línea con lo mencionado en el punto anterior, los ciberdelincuentes han perdido el miedo a lanzar sus ataques contra entidades que, por repercusión pública o por recursos disponibles, son susceptibles de disponer de medios para detener el ataque, revertir sus efectos e incluso, tratar de contraatacar. Pero ello no ha sido impedimento para que estos grupos hayan cometido sus fechorías a lo largo y ancho del planeta, hasta tal punto que el Presidente Biden ha amenazado[2] a algunos paises con represalias si no toman medidas para impedir que estos ciberataques se produzcan desde su territorio, e incluso, esponsorizados por algunos estados.

3. **BENEFICIOS:** si los ataques de ransomware originales recaudaban unos pocos Bitcoins por cada víctima que se sometía al pago del rescate, en la actualidad los rescates que se exigen son tremendamente abultados. Según algunas fuentes, la operadora de oleoductos Colonial pagó casi 5 millones de dólares a los ciberdelincuentes para recuperar la operación de sus sistemas. Esto supone un problema añadido al intrínseco a pagar un rescate, y es que dota a los ciberdelincuentes de fondos para mejorar sus productos, contratar personal experto y ampliar sus operaciones. Es decir, cada vez que se paga un rescate por un ataque de ransomware se está **'alimentando al monstruo'**.

4. **ESPECIALIZACIÓN:** en el sector del ransomware, los actores implicados están cada vez más especializados. Hay grupos de ciberdelincuentes especializados en recopilar la información necesaria de las potenciales víctimas, de cara a facilitar el trabajo de quienes diseñan el ataque; otros grupos se especializan en diseñar el software de incursión en los sistemas de las potenciales víctimas (*dropper*); y finalmente, tenemos al grupo de ciberdelincuentes que crean el ransomware (*payload*), lo operan, y cobran el rescate en criptomonedas muy difíciles de rastrear.

5. **ORGANIZACIÓN:** hasta tal punto llega el nivel de especialización de estos grupos de delincuencia organizada digital que han llegado a crear una industria que podemos calificar de Ransomware-as-a-Service (RaaS), donde cada uno de los actores ofrece sus servicios a otros actores en busca del máximo beneficio mutuo. Y este hecho ha producido, incluso, que alguna de estas plataformas de RaaS haya creado un **código ético** [4] para aquellos que deseen hacer uso de sus servicios para delinquir. En este caso, la noticia surgió cuando la plataforma Darkside publicó un código ético sobre a qué organizaciones no se podía atacar usando su plataforma, para evitar dañar a entidades como hospitales, ONGs, etc. Una iniciativa que recuerda al 'Código de la Piratería' de los siglos XVII y XVIII, y que resultaría risible si no fuera por lo grave que es el problema del ransomware en la actualidad. Estamos ante una verdadera industria con un clarísimo y beneficioso modelo de negocio [5].

CONTINÚA EN PRÓXIMA PÁGINA

6. **BRANDING:** donde hay negocio, y como ocurre también en otros negocios ilegales como el tráfico de drogas, surge lo que podríamos llamar 'reconocimiento de marca'. En este caso, de determinadas plataformas RaaS, como es el caso de Darkside, eGregor o Shark, ya que cuando quienes quieren lanzar un ataque de este tipo ven el éxito que otros están teniendo usando este tipo de plataformas, por una fracción del coste que tendría desarrollarlo todo ellos mismos, les resulta muy fácil la decisión. Es exactamente el mismo razonamiento que ha popularizado todos los servicios en modo de pago por uso: no invierto, sino que sólo pago por lo el uso que hago de un bien o servicio propiedad de otro.

Como ha ocurrido en otros sectores y productos, es previsible que algunas plataformas de ransomware se popularizarán tanto que sacarán del mercado a otras menos competitivas, y comenzarán a mover unas cantidades insultantes de dinero en criptomonedas. Por esa razón, se cree que las organizaciones criminales 'clásicas', de las que se dedican al tráfico de drogas, armas o personas, pueden estar detrás de varias de estas plataformas de RaaS. Y no olvidemos tampoco a ciertos grupos de ciberdelincuentes patrocinados por ciertos estados.

En este entorno, y con el nivel que ha alcanzado la amenaza, la situación ha de ser afrontada a través de importantes esfuerzos de las fuerzas policiales y agencias de inteligencia. Como en otros negocios sucios, el dinero del ramsomware ha de ser cambiado en monedas nacionales para poder comenzar su proceso de blanqueo, y de ese hilo tiran los cuerpos policiales para tratar de desmantelar estas redes de ciberdelincuentes. Y aunque no es para nada una tarea fácil, de la colaboración **de todos** se terminan consiguiendo ciertos éxitos [6], que aunque insuficientes, permiten albergar esperanzas de acabar con esta lacra, o al menos, reducir su impacto todo lo posible.

REFERENCIAS

[1] https://tecnologiaysentidocomun.com/ipages/flipbook/revista-tysc01-octubre-2020 págs. 10-12
[2] https://cnnespanol.cnn.com/2021/07/09/biden-putin-ciberataques-ransomware-trax/
[3] https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html
[4] https://slate.com/technology/2021/05/colonial-pipeline-darkside-ransomware.html
[5] https://blog.trendmicro.com/outsourcing-crime-how-ransomware-as-a-service-works
[6] https://www.csoonline.com/article/3608368/egregor-ransomware-takes-a-hit-after-arrests-in-ukraine.html

MGEIT® MPPM®

eGob®

BPM + ISO 19510
Business Process Management
Gestión de Procesos de Negocio

CERTIFÍCATE EN PROCESOS

Si quieres aportar valor al negocio comienza por Descubrir, Modelar, Implementar, Automatizar y Mejorar sus Procesos de Negocio con Busines Process Management BPM. Además la Gestión por Procesos es el origen del resto de Buenas Practicas relacionadas con Proyectos, Servicios, Productos o Riesgos pues todas ellas se basan exactamente en Procesos.

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Cursos de Doble Certificación convalidables por asignaturas de los Masters MasterGEIT® y/o MasterPPM®.

CONVOCATORIAS 2022/23

- **SEPTIEMBRE 2022 (Formato Martes y Jueves Tardes)**
  Martes 20, jueves 22, martes 27 y jueves 29
- **OCTUBRE 2022 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 21, sabado 22, viernes 28 y sábado 29
- **FEBRERO 2023 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 3, sabado 4, viernes 10 y sábado 11

eGob

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es

La concienciación en ciberseguridad

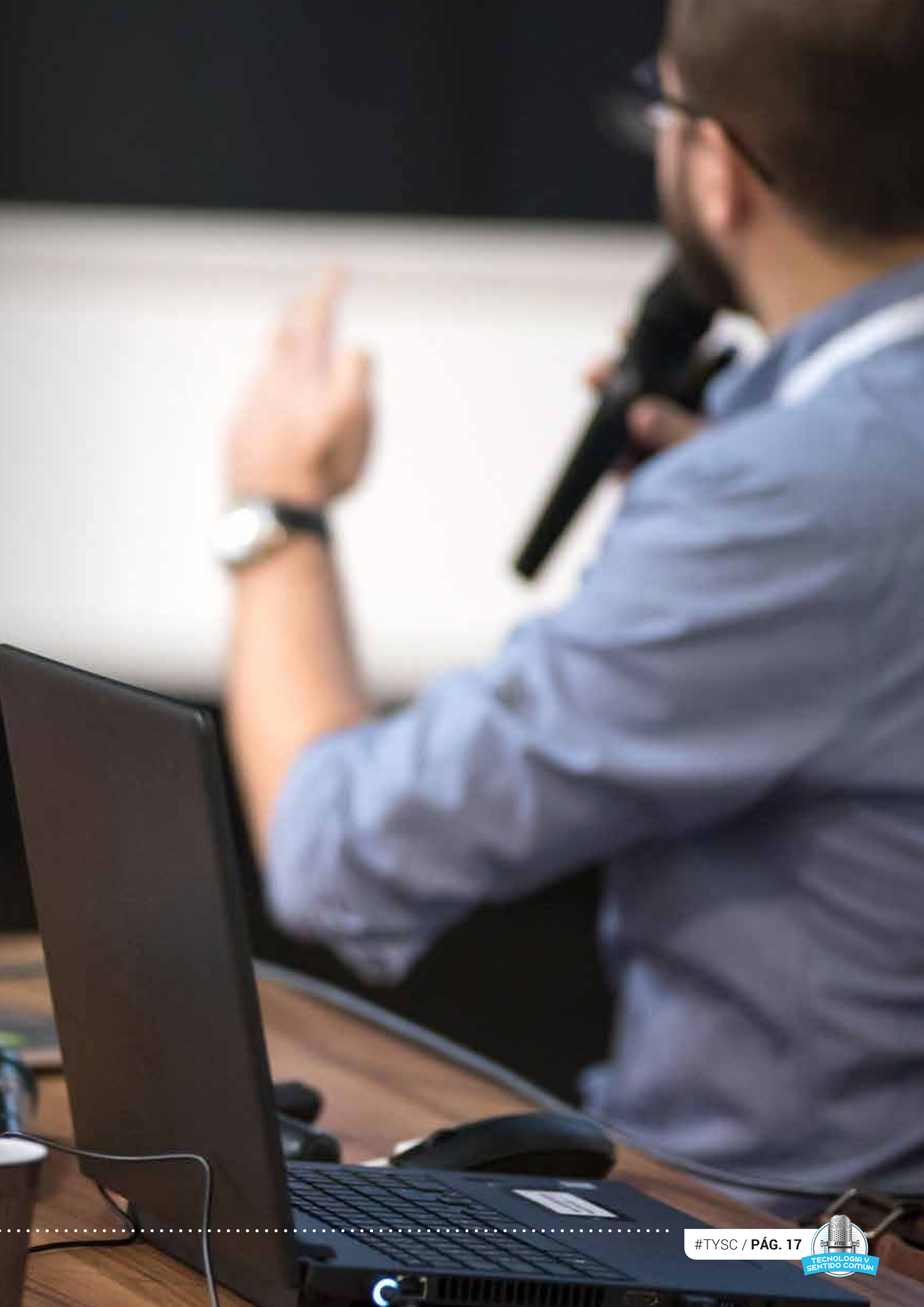
El mes de octubre se celebra, desde hace unos años, el European Cybersecurity Month, un evento destinado a concienciar a ciudadanos y empresas de la importancia de la ciberseguridad para una sociedad digitalizada plenamente productiva y segura. Pero, ¿qué más se está haciendo para que en la ciudadanía cale el mensaje, dado el elevado grado de penetración de determinadas tecnologías en su seno?

"La ciberseguridad empieza por uno mismo". "El usuario es el eslabón más débil en la cadena de la ciberseguridad". "De la colaboración de todos nacen los éxitos contra la ciberdelincuencia". Algunas de estas frases han sido vertidas por quien suscribe, en diferentes artículos de Tecnología y Sentido Común y en otros ámbitos. Todas estas afirmaciones asignan cierto grado de responsabilidad, al respecto de la protección de los sistemas de información, en los usuarios de los mismos. Cualquier persona tendrá una opinión sobre el grado de verosimilitud de estas afirmaciones, pero seguro que coincidiremos en que, para pedir responsabilidad a los usuarios de un sistema, primero hay que formarles, o al menos concienciarles, sobre la forma correcta de su uso y de las repercusiones de hacer un mal uso o de no mantenerlos en adecuadas condiciones.

La digitalización de esta Sociedad se ha acelerado en los últimos años, y en paralelo, han crecido todo tipo de ciberdelitos. En muchas ocasiones, la ciudadanía y las empresas han aprendido sobre ciberseguridad a base de sufrir las consecuencias o el impacto de ataques o estafas que utilizan en todo o en parte el medio digital para su realización. Y en esa situación, ¿es exigible a los poderes públicos una reacción, más allá de la acción represiva (y reactiva) de los Fuerzas y Cuerpos de Seguridad del Estado y de la Administración de Justicia. **Indudablemente, sí**. En primer lugar, porque ese enfoque es insuficiente, ante las dificultades de realizar investigaciones en un marco transfronterizo, y donde en ocasiones son los propios gobiernos de algunos países quienes patrocinan o toleran esa ciberdelincuencia. Y en segundo lugar, porque igual que en otros aspectos de nuestra vida social, como la salud, los gobiernos pueden orientar las estrategias preventivas de la ciudadanía para evitarles perjuicios futuros.

Sin lugar a dudas, la ciberseguridad básica debe formar parte de los currículos académicos en secundaria, formando parte de las competencias tecnológicas que se imparten a los jóvenes actualmente. Pero no hay duda de que la sociedad se protege con un gran retraso ante las amenazas que suponen los diferentes escenarios de ciberdelincuencia, sobre todo si se ha de esperar a que esos jóvenes crezcan con la ciberseguridad personal 'de serie' para incorporarla a empresas y organismos públicos.

CONTINÚA EN PRÓXIMA PÁGINA



De ahí la imperiosa necesidad de que los poderes públicos de todo el planeta, más cuanto más digitalizada esté su sociedad, acometan campañas de concienciación ciudadana sobre el tema, y creen organismos o unidades que trabajen tanto en la línea de la represión del cibercrimen, a través de la colaboración internacional, como en la línea de la prevención del mismo, en base a campañas de concienciación enfocadas en diferentes grupos sociales específicos. Además, por qué no decirlo, también será de recibo que las organizaciones privadas e individuos aporten su granito de arena para colaborar en este objetivo estratégico de reducir al máximo el cibercrimen.

¿Qué se está haciendo en este ámbito en España? La verdad es que para nuestro país podemos decir que se están haciendo bastantes cosas, desde diferentes instancias.

A nivel europeo, la **Agencia Europea de Ciberseguridad (ENISA)**, con sede en Atenas (Grecia), realiza múltiples actividades de concienciación, a través de sus webs, las más significativa de las cuales es la celebración del European Cybersecurity Month[1] en el mes de octubre, desde 2012. Las diferentes páginas web de este organismo están repletas de recursos útiles en el tema de la ciberseguridad, pero también en cuestiones de privacidad. Además, ENISA mantiene un interesante grupo de trabajo internacional para el crecimiento de la concienciación en ciberseguridad *(Ad-Hoc Working Group on Awareness Raising)*.

A nivel nacional en España, contamos con al menos dos entidades que trabajan las cuestiones de concienciación, en dos ámbitos claramente diferenciados:

• **El Centro Criptológico Nacional (CCN)**, unidad del Centro Nacional de Inteligencia, dependiente del Ministerio de Defensa, que centra su área de actuación en las Administraciones Públicas, y cuya actividad alrededor del Esquema Nacional de Seguridad y de la certificación de productos de seguridad es encomiable.

• El **Instituto Nacional de Ciberseguridad (INCIBE)**, sociedad dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, que centra su actividad en las empresas, sobre todo las PYMEs, y la ciudadanía en general. De esta entidad me gustaría destacar la creación de una línea telefónica de atención en materia de ciberseguridad, el 017, y la iniciativa Cibercooperantes, a través de la que se reclutan personas que estén en dispuestas a colaborar en la tarea de concienciación a través de charlas y otras actividades a diferentes colectivos, como escolares o personas mayores.

A nivel autonómico, son muchas las comunidades que tienen iniciativas al respecto, sobretodo enfocadas en la población más joven. Tal es el caso del Centro de Ciberseguridad de la Comunidad Valenciana[2] (CSIRT-CV), referente en el sector por su antigüedad y buen hacer, que desde hace bastantes años mantiene activo un programa de visitas a colegios e institutos de secundaria, en las que los expertos de la entidad tratan de concienciar a los asistentes (padres incluidos) en la materia.

También son muchas las asociaciones, administraciones locales, colegios profesionales o empresas que realizan iniciativas al respecto a lo largo y ancho del país, ya que todo esfuerzo es bienvenido cuando estamos tratando de proteger nuestros equipos y redes de la ciberdelincuencia. Y porque igual que desde pequeños nos enseñan a no cruzar en rojo, porque podemos tener un accidente, o a no aceptar caramelos de desconocidos al salir del colegio, alguien ha de tomar la responsabilidad de explicar a esta Sociedad que la digitalización tiene sus riesgos, y que deber tener cuidado 'ahí afuera'. Yo ya me he enrolado en esta singladura. ¿Y Ud.?

REFERENCIAS

[1] https://cybersecuritymonth.eu/
[2] https://news.itsmf.es/csirt-cv-el-centro-respuesta-a-incidentes-de-ciberseguridad-de-la-comunidad-valenciana/

MGEIT® MPPM®

eGob®

OpenPM² (PjM) + ISO 21502
Project Management
Gestión de Proyectos

CERTIFICATE EN PROYECTOS

La Gestión de Proyectos es la vía natural con la que implementar cambios en las organizaciones. Por encima de la ejecución de actividades una adecuada Gestión de Proyectos permite tener bajo control y garantizar aspectos tan importantes como plazos, costes, riesgos y beneficios ofreciendo información confiable a quien la necesita.

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Cursos de Doble Certificación convalidables por asignaturas de los Masters MasterGEIT® y/o MasterPPM®.

CONVOCATORIAS 2022/23

- **SEPTIEMBRE 2022 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 16, sabado 17, viernes 23 y sábado 24
- **OCTUBRE 2022 (Formato Martes y Jueves Tardes)**
  Martes 18, jueves 20, martes 25 y jueves 27
- **NOVIEMBRE 2022 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 18, sabado 19, viernes 25 y sábado 26

eGob®

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es

EIDAS-2 y la identidad basada en Blockchain

El 3 de junio de 2021 fue publicada la propuesta de Reglamento europeo para modificar el vigente Reglamento eIDAS, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, que ya ha cumplido 7 años. La más interesante novedad de la propuesta de nuevo reglamento es la posibilidad del uso de Blockchain como mecanismo de gestión de la identidad, cuestión que merece de un cierto nivel de análisis.

En mi artículo del mes de diciembre de 2020 de esta publicación[1] se desgranaban algunas de las posibilidades que el uso de cadenas de bloques podían ofrecer a diferentes segmentos del mercado, y una de esas opciones era la gestión de identidades de las partes implicadas en una transacción electrónica. Contamos en España con excelentes profesionales del sector, como Ignacio Alamillo, casualmente entrevistado en el mismo número de Tecnología y Sentido Común, que llevan tiempo apostando por que este tipo de soluciones estén recogidas en la normativa europea, y por lo que parece, con la propuesta de nuevo reglamento eIDAS-2 están mucho más cerca de que ese hecho se convierta en realidad.

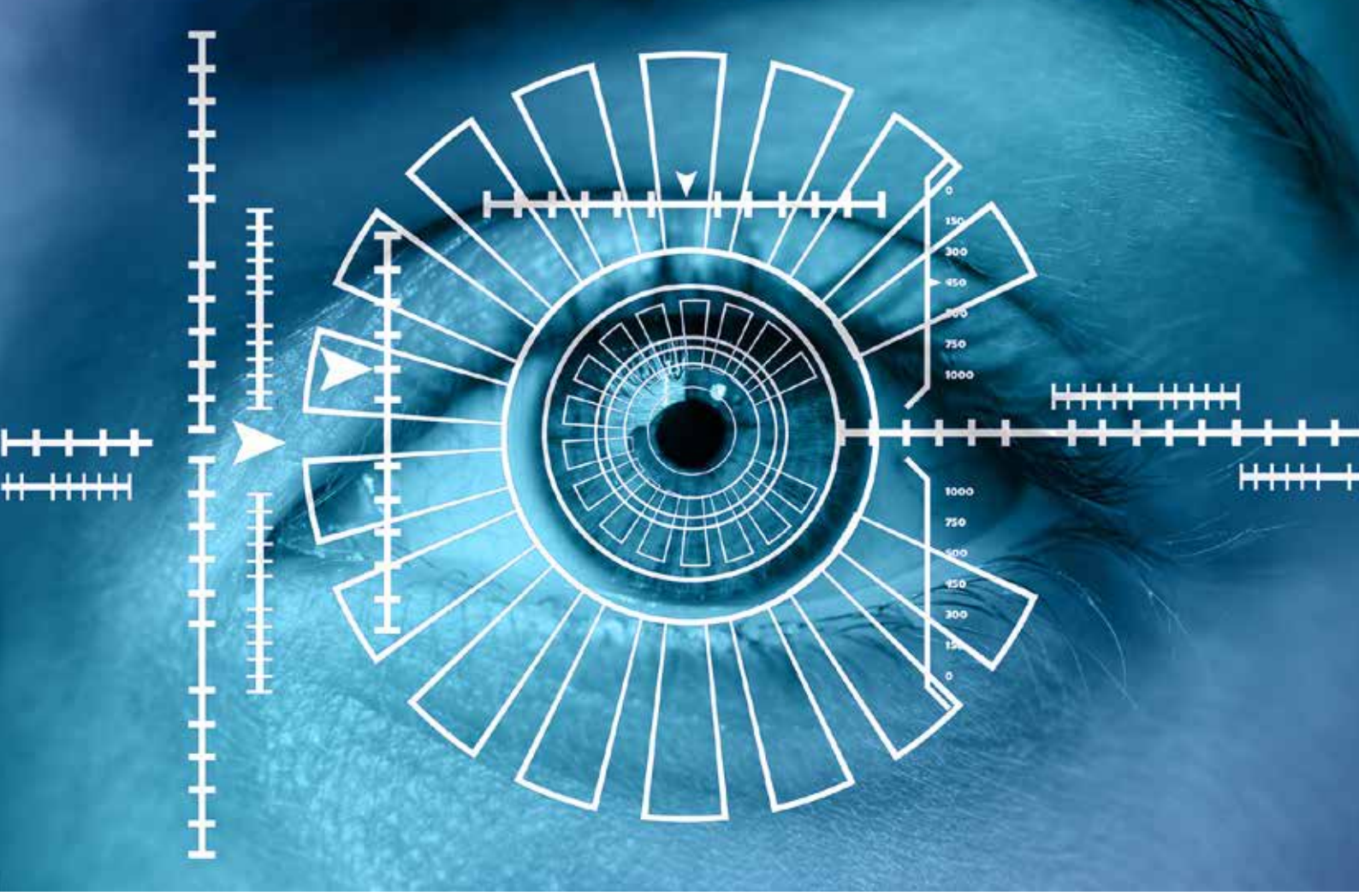
En 2014, el Parlamento y el Consejo de la Unión Europea aprobaron el Reglamento (UE) nº 910/2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Al ser un Reglamento Europeo, no necesitó de trasposición a las leyes de cada país miembro, pese a lo cual en España se pensó en que era necesaria una norma, la Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza, para complementar a dicho Reglamento.

En esencia, eIDAS trataba de eliminar barreras entre países europeos miembros, facilitando la interoperabilidad entre sistemas de identificación de ciudadanos y de verificación de la validez de sus firmas digitales. Todo ello, con el objetivo de permitir operar con mayor facilidad y menor coste, aumentando la eficacia de los servicios on line, públicos o privados, potenciando el comercio electrónico en el territorio europeo (Mercado Único Digital). Para ello, el Reglamento evolucionaba el armazón legal previo de la Directiva 1999/93/CE, a la que derogaba, permitiendo aspecto como el reconocimiento mutuo de identidades entre países miembros en el uso de servicios públicos electrónicos, definiendo los aspectos relativos a la validez de los diferentes tipos de firma electrónica, o los diferentes servicios en los que se han de basar los servicios electrónicos bajo el alcance del Reglamento (eSignature, eSeal, eDelivery, o eTimestamp).

En España, el servicio CL@VE es el que proporciona información acerca de las identidades digitales españolas a cualquier entidad pública europea, merced a su nodo eIDAS, y que a través de la red SARA conecta con la red europea sTESTA (secure Trans-European Services for Telematics between Administrations).

Tras siete años de vigencia, la UE decidió proponer el pasado 3 de junio de 2021 un nuevo Reglamento eIDAS-2, que supone un cambio de paradigma en una cuestión clave: en lugar de requerir la interoperabilidad entre sistemas de identificación transfronterizos, permite el derecho de los ciudadanos europeos a disponer, de forma voluntaria y gratuita, de una identidad digital europea (e-ID) que pueda usar en cualquier servicio electrónico del mercado europeo. Esta propuesta llega después de los decepcionantes resultados del Reglamento eIDAS por lo que a conseguir la interoperabilidad se refiere, ya que sólo hay 15 sistemas de identificación conectados, que cubren únicamente al 59% de la población europea.

CONTINÚA EN PRÓXIMA PÁGINA



La segunda novedad más importante es la posibilidad de que los sistemas de identificación y firma no requieran de una tercera parte de confianza, como ocurre con los sistemas basados en certificados digitales que hemos estado utilizando hasta el momento, sino que pueda basarse en sistemas de identificación y firma autosoberanos basados en Blockchain[2]. En este aspecto, en España contamos con varios de los mayores expertos europeos en la materia, y es necesario hacer notar que la propuesta para el eIDAS-2 se basa, fundamentalmente, en un estudio que varios de estos expertos han realizado por encargo de la Comisión Europea. Además, es nuestro país el que más prestadores de servicios de confianza tiene.

La Comisión espera que, merced a este nuevo Reglamento aún no aprobado, en 2030 el 80% de los ciudadanos europeos dispongan de una e-ID a través de los llamados European Digital Identity Wallets, que cualquiera podrá llevar en su teléfono inteligente, y con los que se dispondrá de acceso no sólo a los servicios del sector público europeo, sino que pueda usarse también en transacciones privadas.

¿Qué implicaciones tiene la posibilidad de poder utilizar sistemas Blockchain para almacenar la identificación y firma legalmente válidas de una persona? En primer lugar, este cambio legal se basa en la existencia de sistemas que permiten la conocida como Self-Sovereign Identity, en la que son los propios ciudadanos los dueños de sus datos de identidad y los responsables de su gestión. En 2016, Naciones Unidas arrancó la Alianza ID2020 con varias partes interesadas, con el objetivo de asegurar que, en el marco de los Objetivos de Desarrollo Sostenible, se podía proporcionar identidades digitales para cualquier persona de forma universal y ética, satisfaciendo los requisitos de las 4 P's: privada, portable, persistente y personal. Los sistemas que den soporte a estas iniciativas no han de poder ser falsificados, y dado que esa es una de las características de Blockchain, esta tecnología es un soporte adecuado para ello.
Lo que la UE hace, al abrir esta posibilidad, es plantear un futuro en el que convivan los sistemas de identificación y firma digital 'clásicos', proporcionados por determinados prestadores de servicios de confianza, y sistemas que se alineen con los objetivos marcados por Naciones Unidas a este respecto.

REFERENCIAS

[1] https://tecnologiaysentidocomun.com/ipages/flipbook/revista-tysc03-diciembre-2020 págs. 10-12
[2] https://diariolaley.laleynext.es/dll/2021/06/24/la-propuesta-de-reglamento-eidas-2-la-identidad-digital-autosoberana-y-la-regulacion-de-blockchain
[3] https://www.frontiersin.org/articles/10.3389/fbloc.2021.616779/full

MGEIT® MPPM®

eGob®

OpenPM² (PgM) + ISO 21503
Programme Management
Gestión de Programas

CERTIFICATE EN PROGRAMAS

La Gestión de Programas de Proyectos es responsable de que los resultados de los proyectos se conviertan en beneficios, mientras que los Proyectos finalizan con la entrega de sus resultados, los Programas quedan aportando valor al negocio más allá de la vida de cada proyecto. Si quieres de verdad lograr beneficios certificate en Gestión de Programas.

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones de 5 horas en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Cursos de Doble Certificación convalidables por asignaturas de los Masters MasterGEIT® y/o MasterPPM®.

CONVOCATORIAS 2022/23

- **NOVIEMBRE 2022 (Formato Martes y Jueves Tardes)**
  Martes 15, jueves 17, martes 22 y jueves 24
- **ENERO 2023 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 20, sabado 21, viernes 27 y sábado 28

eGob®

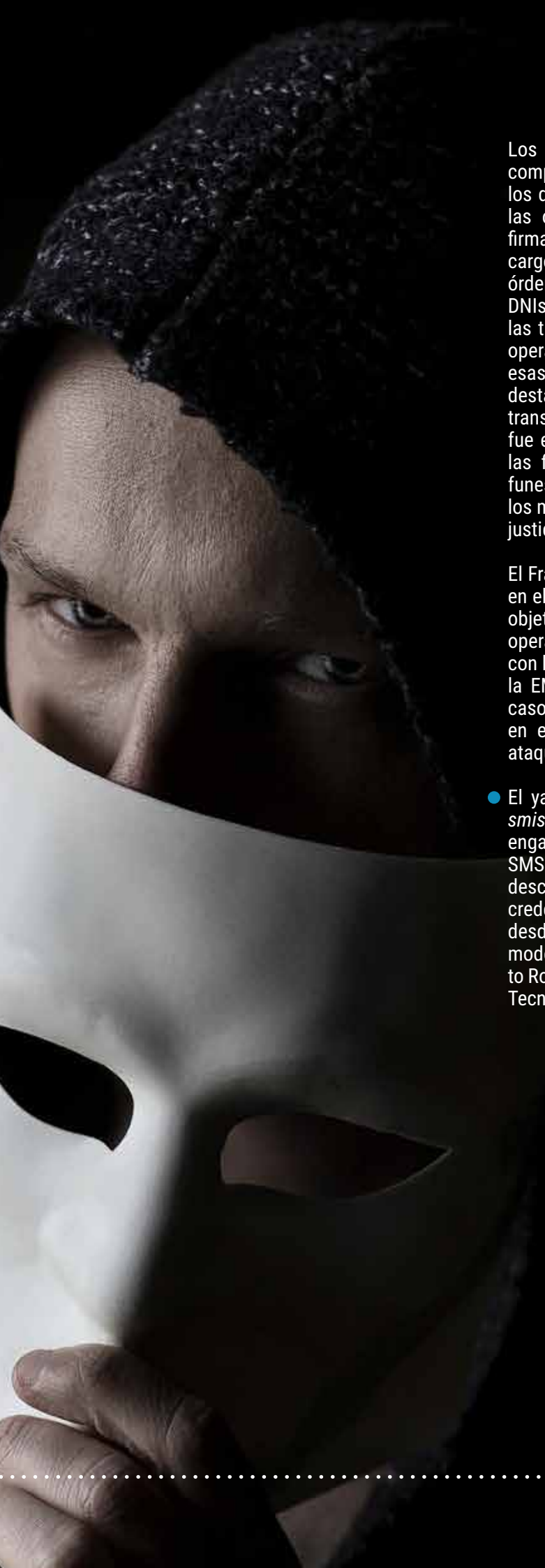
Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es

Qué es y cómo protegerse de la amenaza de la Ingeniería Social (I)

Aunque cada vez los ataques dirigidos a las organizaciones son técnicamente más sofisticados, en un buen porcentaje de ellos hay una componente de engaño a los seres humanos que utilizamos los sistemas de información de todo tipo. Los ciberdelincuentes conocen la Ingeniería Social y la aprovechan, razón por la cual se ha afrontar esta amenaza.

En septiembre de 2019, una directiva financiera de una compañía de transporte recibió una llamada telefónica en la que una persona, identificándose como abogado de una gran consultora internacional, en un perfecto castellano sin acento alguno, le informaba de una operación financiera confidencial que la compañía iba a poner en marcha y que se anunciaría a los medios unos días después, cuando estuviese cerrada completamente. El llamante informó a la directiva que esa operación estaba capitaneada por el presidente de la compañía, y que éste le daría las oportunas instrucciones en breve, pero que ella, como participante en la operación debía firmar antes un compromiso de confidencialidad. Un rato después, recibió un correo electrónico (falso) del presidente de su empresa, preguntándole si había contactado con ella un abogado por un tema confidencial, y dándole instrucciones de que realizara cuanto éste le indicara. Tras una serie de intercambio de documentos, y firmas de varias personas de la empresa en órdenes de pago, la compañía terminó transfiriendo a una cuenta en Hong Kong una importantísima cantidad de dinero que debía servir para esa operación confidencial. Pero resultó que no había nada de nada, todo era un engaño y los delincuentes que lo pergeñaron movieron rápidamente el dinero y desaparecieron. Cuando la compañía quiso darse cuenta, todo se había perdido, aunque hubo cierta suerte, ya que el montante que los estafadores habían planteado recibir de la compañía era muy superior.

Éste es un caso real [1]. La compañía afectada fue la Empresa Municipal de Transportes de Valencia (España), y la cantidad de dinero estafada ascendió a más de 4 millones de euros, provocando un enorme revuelo mediático en la ciudad, y con la directiva despedida y acusada de los delitos oportunos. El banco tampoco parece que saliera bien parado, al menos en su reputación y operativa. Este caso es un ejemplo paradigmático y de estudio de lo que se conoce como **Fraude al CEO**, porque tiene todos los ingredientes típicos de este tipo de ataques, que mezclan los mecanismos clásicos de la estafa con partes basadas en los sistemas de información: confidencialidad, relaciones de poder, apariencia de credibilidad, miedo al despido si se incumple una supuesta orden del superior jerárquico, urgencia, falsa confianza, y falsificación de documentos y otras informaciones. La directiva de nuestro caso recibió un correo del presidente de la compañía desde un aparente dominio existente, pero realmente lo recibió desde una cuenta falsa de otro dominio, gracias a las facilidades que algunos clientes de correo electrónico dan para que estas cosas ocurran.



Los delincuentes utilizaron la firma de la directiva en el compromiso de confidencialidad para comenzar a preparar los documentos que enviarían posteriormente al banco para las órdenes de transferencia, pero les hacían falta otras firmas, así que pidieron copia de los DNIs de otros altos cargos, y teniendo en cuenta que la directiva creía que recibía órdenes del cargo más alto de su empresa, obedeció. De esos DNIs se obtuvieron las firmas necesarias para poder tramitar las transferencias como cartas de pago, y no a través de la operativa digital del banco, ya que eso hubiera exigido que esas personas validaran las transferencias, lo cual habría destapado de raíz la estafa. El banco, al recibir las órdenes de transferencia con las firmas de los autorizados para hacerlas, fue ejecutándolas pese a haber una discrepancia en una de las firmas. Finalmente, toda la situación se destapó, con funestas consecuencias para los participantes, excepto para los malhechores, que no han sido puestos a disposición de la justicia ni el dinero ha sido recuperado.

El Fraude al CEO es uno de las variantes de lo que se conoce en el argot de la ciberseguridad como Ingeniería Social, cuyo objeto es, fundamentalmente, hackear a los humanos que operan el sistema que se desea violentar para que colaboren con los delincuentes. El sistema atacado, como en el caso de la EMT, no necesariamente ha de ser informático. En este caso, se atacó al procedimiento de pagos, algo muy habitual en estos casos. Pero hay más ejemplos de este tipo de ataques:

- El ya archiconocido *phishing*, que junto con sus primos *el smishing y el vishing* conforman una triada perfecta del engaño a los usuarios del correo electrónico o receptores de SMS. Pedirles que hagan clic en un enlace malicioso, o que descarguen una aplicación maliciosa, o que introduzcan sus credenciales bancarias en una formulario al que se accede desde un cómodo enlace del correo electrónico, son los modos habituales de este engaño. Nuestro compañero Alberto Rodríguez escribió un aclaratorio artículo en el número 3 de Tecnología y Sentido Común, en diciembre de 2020.

CONTINÚA EN PRÓXIMA PÁGINA

- La llamada del soporte de Microsoft [3]: aprovechando que el sistema operativo de la compañía de Redmond está en muchísimos ordenadores, y que muchas organizaciones tiene externalizado el soporte técnico a usuarios, el malhechor llama por teléfono y se hace pasar por un técnico de soporte de Microsoft y le dice al usuario que han detectado un problema en su equipo y que debe dejarle acceso remoto a su PC para solucionarlo. Cuando el usuario descarga la aplicación de control remoto y da acceso al delincuente, éste le pone un protector de pantalla y comienza a realizar sus maldades: robo de información personal, instalación de malware, acceso a sistemas internos de la compañía, etc. También se realiza sin citar a Microsoft.

- El cambio de cuenta corriente de pago de facturas [4]: haciéndose pasar por el departamento de Administración de un proveedor, se solicita un cambio de cuenta en el que pagar las facturas a ese proveedor. La empresa atacada paga en esas cuentas hasta que la empresa que debía recibir el dinero se queja. Las Administraciones Públicas españolas han sufrido bastantes ataques de este tipo debido a la abundante información sobre sus contratos en la Plataforma de Contratos del Sector Público. Un ejemplo de cómo la transparencia puede poner en peligro el servicio público. También de otras fuentes de información, como LinkedIn por ejemplo [5], se pueden obtener datos que faciliten el contacto con quien puede realizar este tipo de cambios en los ERP de las organizaciones.

- La doncella maliciosa: o *Evil Maid*, es un ataque en el que una delincuente se hace pasar por servicio de limpieza en hoteles u oficinas para clonar o sustraer información de los equipos informáticos de las víctimas. Aquí la engañada es la empresa que la contrata, si es que hay contratación, pero la víctima es otra que, además, en muchas ocasiones no se entera de lo que ha ocurrido.

Etc.
En el próximo número de Tecnología y Sentido Común analizaremos la raíz y fundamentos psicológicos de este tipo de ataques, la creatividad de sus autores, y daremos unas pinceladas de cómo tratar de evitarlos.

REFERENCIAS

[1] https://www.eldiario.es/comunitat-valenciana/llamada-fabulosa-millones-emt-valencia_1_1243386.html
[2] https://tecnologiaysentidocomun.com/ipages/flipbook/revista-tysc03-diciembre-2020 páginas 18 a 21
[3] https://docs.microsoft.com/es-es/windows/security/threat-protection/intelligence/support-scams
[4] https://elpais.com/espana/2021-02-10/el-ayuntamiento-de-valencia-denuncia-un-fraude-de-21000-euros-en-el-palacio-de-congresos.html
[5] https://www.elladodelmal.com/2021/11/linkedin-y-la-eleccion-de-la-victima.html

MGEIT® MPPM®

eGob®

FitSM + ISO 20000
Service Management
Gestión de Servicios de Tecnología

CERTIFICATE EN SERVICIOS

Estamos en un mundo cada vez más "As-a-Service" donde todo se comercializa como servicio con la ayuda de las nuevas tecnologías, pero las tecnologías que soportan los servicios deben ser adecuadamente gestionadas para dotarlas de capacidad, continuidad, disponibilidad, seguridad y resiliencia. Si quieres prepararte para la Era Digital fórmate en Servicios.

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Cursos de Doble Certificación convalidables por asignaturas de los Masters MasterGEIT® y/o MasterPPM®.

CONVOCATORIAS 2022/23

- **SEPTIEMBRE 2022 (Formato Martes y Jueves Tardes)**
  Martes 6, jueves 8, martes 13 y jueves 15
- **ENERO 2022 (Formato Martes y Jueves Tardes)**
  Martes 17, jueves 19, martes 24 y jueves 26

eGob®

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es

Qué es y cómo protegerse de la amenaza de la Ingeniería Social (II)

En el número del mes pasado de Tecnología y Sentido Común comenzamos una serie de artículos sobre la amenaza que representan los ataques basados en Ingeniería Social, y se expusieron algunos ejemplos representativos de las tipologías de estos ataques. En el artículo de este mes, continuamos la serie profundizando en las características principales de los ataques de Ingeniería Social.

En mi artículo del mes de enero de 2022 de esta publicación[1] se introdujeron algunos ejemplos paradigmáticos y sucesos reales de ataques basados en técnicas de Ingeniería Social. La característica fundamental básica de estos ataques es que se enfocan en la parte humana del sistema que se desea atacar. Por tanto, nos encontramos ante un tipo de amenaza al componente no tecnológico de los sistemas de información o de los procesos económicos, y por tanto, las estrategias para evitar o mitigar este tipo de amenazas han de pasar necesariamente por comprender su base psicológica o social, y por la implantación de medidas organizativas, a través de las correspondientes acciones de concienciación, aunque también hay ciertas medidas tecnológicas que pueden ayudar a evitar que estos ataques tengan éxito.

En primer lugar, hay que saber que un ataque de ingeniería social bien urdido va precedido de un proceso de recopilación de información sobre la entidad y/o personas que van a ser atacadas, mediante técnicas de Inteligencia de Fuentes Abiertas (OSINT), temática de alto interés para conocer cómo trabajan los delincuentes de este tipo. Según algunos autores [2], podemos distinguir diferentes tipos de actores que hacen uso de las técnicas de Ingeniería Social, entre los cuales podemos citar todo tipo de hackers, espías, estafadores, reclutadores o vendedores. Es obvio que las técnicas de Ingeniería Social no son delictivas en sí mismas, pero sí pueden serlo los resultados de su aplicación. Por ejemplo, no está prohibido rebuscar en la basura (*trashing*, en el argot de la ciberseguridad), pero si de los datos obtenidos de ese procedimiento se realiza una suplantación de identidad, se estará cometiendo un presunto delito.

Algunas de las técnicas de Ingeniería Social disponibles son muy simples, incluso infantiles, pero todas ellas pueden ser perfectamente válidas en diferentes entornos o situaciones.

Huyendo de la terminología inglesa en la materia que las identifica, podemos citar algunas de estas técnicas básicas, orientadas a la fase de recopilación de información:

•Colarse en un edificio o instalación sin autorización, aprovechando que otra persona abre la puerta.
•Rebuscar en la basura.
•Escuchar conversaciones ajenas.
•Observar disimuladamente datos confidenciales, como contraseñas de acceso o pines de tarjetas de crédito.
•Husmear entre las pertenencias de un compañero de oficina, o en sus activos digitales.
•Sobornar directamente a quien tiene la información que queremos.
•Etc.

Durante la fase de ejecución del ataque, los delincuentes utilizarán otro tipo de técnicas, tales como:

•La suplantación de la identidad, haciéndose pasar por otra persona o por un miembro de una determinada organización.
•La suplantación de la dirección IP, registro de DNS o dirección MAC del equipo de la persona atacada o del sistema u organización que se desea atacar, para capturar información confidencial o claves de acceso.
•*Phishing, vishing o smishing* [3], enviando correos electrónicos, realizando llamadas falsas o remitiendo SMS fraudulentos, respectivamente, para tratar que la víctima proporcione la información que los delincuentes necesitan (credenciales de acceso, cuentas bancarias, números de tarjeta de crédito, etc.)

CONTINÚA EN PRÓXIMA PÁGINA

En todo caso, es muy habitual que los delincuentes utilicen una combinación de técnicas de ataque físicas y lógicas, como ocurrió en el caso del fraude a la EMT de Valencia en 2019, comentado en nuestro artículo anterior.

Sin embargo, en la mayoría de los casos de ataques de Ingeniería Social se opera sobre determinados aspectos psicológicos del ser humano, que se convierten en vulnerabilidades de los sistemas atacados si no se está adecuadamente entrenado para ser evitados. Entre estos aspectos psicológicos que los delincuentes aprovechan están los siguientes:

•El apremio, obligatoriedad o urgencia en hacer que algo se nos pide. Se utiliza mucho en ataques de *phishing,* e incluso lo usan algunos vendedores con aquello tan manido de 'esta oferta termina en cuanto Ud. salga por la puerta'.
•El gusto por parecer expertos o por ayudar al prójimo provoca que se utilicen técnicas de elicitación para obtener información valiosa. También se usa en determinados tipos de ataque en los que se apela a la solidaridad o la colaboración ciudadana, como medio de manipulación o persuasión.
•El respeto a la autoridad, o la simpatía, o la amenaza velada, combinados con una suplantación de personalidad, también son utilizados en algunos fraudes para conseguir que la persona atacada realice las acciones que los delincuentes desean.
•Etc.

En nuestro próximo artículo, para finalizar esta serie, nos centraremos en las protección frente a los diferentes técnicas de Ingeniería Social, que en muchos de los casos pasarán por la concienciación de los usuarios de nuestra organización, y por el establecimiento de procedimientos seguros de operación.

Referencias

[1] https://tecnologiaysentidocomun.com/ipages/flipbook/revista-tysc15-enero-2022 págs. 10-12
[2] Hacking con Ingeniería Social. Técnicas para hackear humanos. Antonio Ramos et al. 2015. Editorial RA-MA. ISBN 978-84-9964-539-1
[3] https://tecnologiaysentidocomun.com/ipages/flipbook/revista-tysc03-diciembre-2020 págs. 18-20

MGEIT®

eGob®

CSX + ISO 27000
Information Security
Seguridad de la Información

CERTIFÍCATE EN SEGURIDAD

La Seguridad de la Información y la Ciberseguridad son las asignaturas pendientes en la mayoría de las organizaciones, no obstante, la frecuencia y gravedad de los ataques está obligando a la Alta Dirección a invertir en asegurar la Información y tecnología que da soporte al negocio. Si tu objetivo es estar seguro certificate en seguridad.

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones de 5 horas en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Curso de Doble Certificación del Master de Gobierno y Gestión de Información y Tecnología MasterGEIT®

CONVOCATORIAS 2022/23

- **FEBRERO 2023 (Formato Martes y Jueves Tardes)**
  Martes 7, jueves 9, martes 14 y jueves 16
- **MARZO 2023 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 3, sabado 4, viernes 10 y sábado 11

eGob

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es

Qué es y cómo protegerse de la amenaza de la Ingeniería Social (y III)

En los dos números anteriores de Tecnología y Sentido Común publicamos una serie de artículos sobre la amenaza que representan los ataques basados en Ingeniería Social, se expusieron algunos ejemplos representativos de las tipologías de estos ataques, y se detallaron algunas de las vulnerabilidades que las diferentes técnicas de Ingeniería Social explotan. En el artículo de este mes, finalizamos la serie con las medidas de protección frente a las diferentes técnicas y algunos consejos sobre qué hacer si acabamos siendo víctimas.

En el artículo del mes de enero de 2022 de esta publicación se introdujeron algunos ejemplos paradigmáticos y sucesos reales de ataques basados en técnicas de Ingeniería Social. Seguimos la serie explicando las bases psicológicas y sociales de estos ataques[1], que se enfocan en la parte humana del sistema que se desea atacar. Y en este tercer artículo de la serie vamos a centrarnos en las diferentes medidas que podemos tomar para tratar de eludir estos ataques, o qué hacer si somos víctimas de uno de ellos.

Si hablamos de vulnerabilidades, y nos referimos a un software o sistema, éstas se solucionan con actualizaciones o parches de seguridad. Pero si las vulnerabilidades a las que nos referimos forman parte de la condición humana, y cada uno de nosotros somos más o menos propensos a que se utilicen contra nosotros, la principal medida de protección es el conocimiento de dichas vulnerabilidades. La famosa *awareness*, en inglés. Debemos ser conscientes de que existen este tipo de técnicas para hackear humanos y, cada cual desde su nivel de responsabilidad, debe impulsar las medidas necesarias para minimizar la efectividad de estos ataques.

Por ejemplo, se pueden lanzar campañas de falso phishing para detectar a aquellas personas más proclives a caer en este tipo de engaños a través del correo electrónico, y proporcionarles la formación necesaria para que sean capaces de identificar este tipo de ataques y respondan a los mismos de la forma que se haya establecido en la organización. Concienciación, concienciación y concienciación[2]. Evitar que se haga caso de las campañas de correo fraudulento puede suponer una importante reducción en el riesgo de sufrir robo de información personal o financiera, o un ataque de ransomware.

En los programas de concienciación, hay que formar al personal sobre las actitudes de los atacantes a las que deben prestar atención:

•Nerviosismo y sensación de urgencia.
•Amenazas más o menos explícitas.
•Mentiras o inexactitudes.
•Cambio de versión de la 'historia'.
•Terminología o palabras que no se ajustan a la realidad de la organización.
•Etc.

CONTINÚA EN PRÓXIMA PÁGINA

En el caso de que se detecte alguno de estos comportamientos, el personal debe seguir firmemente los protocolos, normas y procedimientos de la organización, recopilando al mismo tiempo toda la información que pueda de la conversación con el atacante. Cualquier petición que se salga del marco organizativo habitual deberá ser confirmada o contrastada con los superiores correspondientes por un medio diferente al que se ha recibido la misma.

Por ejemplo, si no piden por email cambiar el número de cuenta en el que se abonan las facturas de un proveedor concreto, será muy conveniente hablar por teléfono con el departamento contable o de facturación de dicho proveedor, **usando los datos previamente existentes en nuestros registros**, y no los del correo electrónico en el que se ha recibido la solicitud.

Es importantísimo que nuestro personal sepa que es posible decir 'No' a las solicitudes, cuando esa sea la mejor opción, ante la duda justificada sobre si es una petición legítima o no. Siempre se va a poder recibir de nuevo, y confirmar por otro medio, la petición si ésta es legítima y atenderla si las dudas sobre dicha legitimidad se han resuelto. En estos casos, hay que hacer uso del sentido común.

Si hablamos de organizaciones de cierto tamaño, es imperativo establecer una clasificación de la información que se maneja en cada ámbito, y quienes pueden o no acceder a ella. Cumplir con esta normativa evitará que información confidencial pueda acabar en las manos equivocadas a través de un ataque al personal que la maneja. Igualmente, la política de destrucción de soporte debería permitir evitar que se descubra información de la organización a traés de técnicas de trashing, y las medidas de protección física de las instalaciones y equipos de la organización deberían ser coherentes con la información que se maneje en cada una de ellas.

Pero ¿qué hacemos si ya hemos sido víctimas del ataque y hemos 'picado el anzuelo'? En ese caso, dependerá del ataque sufrido, de los resultados del mismo, y de las consecuencias que tanto el ataque como su recuperación vayan a tener en la persona u organización. A este respecto, la Oficina de Seguridad del Internauta de INCIBE[3] dispone de información importante, en forma de infografías, que deberíamos utilizar en los esfuerzos de concienciación del personal, sobre todo porque hay que evitar que dicho personal, si se ve afectado por uno de estos ataques, se proteja a sí mismo y no informe del incidente, provocando que las consecuencias sean aún peores.

En esencia, lo que hay que hacer en caso de sufrir uno de estos ataques es impedir lo antes posible que empeoren los efectos del mismo, para luego proceder a la fase de recuperación. Dependiendo del tipo de ataque recibido, en una primera fase, es conveniente cambiar contraseñas y revisar el estado de los sistemas de autenticación de doble factor en nuestros servicios en línea que hayan podido ser utilizados por el atacante. También conviene revisar nuestras cuentas bancarias, tarjetas de crédito, etc., para detectar movimientos no realizados por nosotros, y denunciarlo a la entidad bancaria y a las autoridades. En el caso de robo de información, habrá que estar atento a que no se activen perfiles con nuestros datos en redes sociales u otros servicios, que puedan poner en riesgo nuestra reputación o ser utilizados como gancho para cometer otros tipos de ataques contra nuestros conocidos. En caso de detectar estas duplicaciones de perfiles, es crítico denunciarlos rápidamente a los administradores de esos servicios en línea.

En resumen, **concienciación, atención, sentido común y capacidad de reacción** son los cuatro factores que van a permitir minimizar el riesgo y mitigar los efectos ante los diferentes ataques de Ingeniería Social.

REFERENCIAS

[1] https://tecnologiaysentidocomun.com/ipages/flipbook/revista-tysc16-febrero-2022 págs. 10-12
[2] https://tecnologiaysentidocomun.com/ipages/flipbook/revista-tysc13-noviembre-2021 págs. 10-12
[3] https://www.osi.es/es/que-hacer-si-eres-victima-de-un-fraude

MGEIT®

eGob®

CBCI + ISO 22301
Business Continuity
Continuidad del Negocio

CERTIFÍCATE EN CONTINUIDAD

Inundaciones, incendios, robos o pérdida de empleados clave producen las interrupciones más habituales en las organizaciones y pueden y deben evitarse. La continuidad de negocio consiste en tener un plan con el que manejar situaciones difíciles y continuar funcionando con la menor interrupción. SI quieres resiliencia certifícate en continuidad.

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Curso de Doble Certificación del Master de Gobierno y Gestión de Información y Tecnología MasterGEIT®

CONVOCATORIAS 2022/23

- **MARZO 2023 (Formato Martes y Jueves Tardes)**
  Martes 7, jueves 9, martes 14 y jueves 16
- **ABRIL 2023 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 7, sabado 8, viernes 14 y sábado 15

eGob®

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es

OSINT, o qué puede saber cualquiera sobre nosotros

Seguro que todos nuestros lectores han hecho el ejercicio de buscar su nombre en algún buscador, para ver qué aparece. Esta actividad inocente e inocua puede no serlo tanto en determinadas circunstancias, porque hoy en día todos tenemos buena parte de nuestra vida en la Red. ¿Conocemos los riesgos que asumimos? ¿Somos conscientes de toda la información que propocionamos en Internet? ¿Cómo alguien puede aprovecharse de nuestra 'locuacidad online'?

En el mes pasado terminé una serie de artículos para Tecnología y Sentido Común acerca de la amenaza que supone la Ingeniería Social en un mundo digitalizado. Una parte importante del éxito de algunos de los tipos de ataques que se basan en técnicas de Ingeniería Social depende de la cantidad y calidad de la información disponible del objetivo a atacar. Esa información puede estar disponible al inicio de la fase de preparación del ataque, pero puede también ir recabándose mientras en las diferentes fases del mismo, conforme el ataque se desarrolla y se conoce mejor al objetivo.

Al conjunto de técnicas por las que un agente recopila información acerca un objetivo a través de fuentes abiertas y/o públicas se le suele denominar OSINT (*de Open Source Intelligence*). Unas actividades que se han visto muy facilitadas por el auge de Internet y las redes sociales, por motivos que, aunque son obvios, a pocas personas parecen preocuparles:

•Las personas publican en sus redes sociales detalles de sus vidas, en ocasiones, íntimos, acompañados de fotografías.
•Las organizaciones y administraciones públicas utilizan tanto Internet como las redes sociales para promocionar sus actividades o publicar información que están obligados a publicar por cumplimiento normativo.
•Hay una percepción en muchas capas de la sociedad de que la intimidad y la privacidad no tienen valor alguno.

CONTINÚA EN PRÓXIMA PÁGINA

¿Qué efecto tienen estas actitudes en el Mundo Real™? Recuerdo que hace unos doce años, en una conferencia a alumnos de instituto, ya les mencioné una web que, con cierto tono acusador, denunciaba estas actitudes como perniciosas, y trataba de concienciar sobre el problema. Se trataba de Please Rob Me[1], servicio que recopilaba información sobre las cosas que se publicaban en redes sociales y que podían dar pistas a los malhechores sobre viviendas o negocios vacíos porque, por ejemplo, sus habitantes o propietarios se habían ido de vacaciones y estaban publicando toda la información en Internet sobre lo bien que lo estaban pasando en Hawaii. ¿Qué podemos aprender de esto? **Si queremos fardar de vacaciones, hagámoslo a la vuelta, escribiendo los *posts* en pasado**. Nuestros *haters* sufrirán igual, nuestros amigos sentirán la misma envidia, pero nuestros bienes y familiares estarán menos expuestos.

Simplemente buscar en un navegador por nuestro nombre no revelará toda la información que un delincuente motivado puede localizar de nosotros de forma totalmente gratuita y bastante sencilla, sea cual sea el tipo de delito del que pretenda que seamos víctimas: robo, suplantación de identidad, estafa, secuestros virtuales, etc. El tema de la suplantación de identidad tiene variantes curiosas en las redes sociales, con las duplicidades de cuentas, que tratan de engañar a nuestros contactos en dichas redes haciéndoles creer, por ejemplo, que hemos perdido el acceso a la red social y que hemos tenido que crear un nuevo perfil, para que nos acepten de nuevo como contactos. No lo crea, y no lo haga. Todas las redes sociales tienen métodos alternativos para recuperar cuentas. Así que si le llega ese tipo de petición, **rechácela y reporte la cuenta fraudulenta**. Si quiere comprobar si realmente su contacto es un poco torpe y realmente ha tenido que crear una nueva cuenta, pregúnteselo por un medio alternativo a la red social, y actúe en consecuencia.

Como decía, hay fuentes de información muy interesantes y que no son muy populares entre los internautas. Por ejemplo, ¿es el lector consciente de toda la información que proporciona una fotografía publicada en una red social? Me estoy refiriendo a los **metadatos de la fotografía**, entre los que está la información EXIF, que contiene datos técnicos sobre la fotografía, además de información de la fecha y hora donde se tomó. Analizar los metadatos de las fotografías que publicamos puede arrojar interesantes conclusiones, si además, la complementamos con la información que nosotros mismos volcamos al publicarlas y la información que la propia red social añade. ¿No sigue apeteciendo que nos etiqueten en fotos ajenas?

Otra fuente de información disponible para los malhechores son los *leaks*, o filtraciones, que brechas de seguridad en servicios on line han permitido que información privada (como números de teléfono, direcciones de email, fecha de nacimiento, dirección postal, e incluso contraseñas) esté a disposición de todos los que deseen utilizarlas, seguramente para el mal. ¿Recibe llamadas desde el extranjero que no espera? ¿Ha aumentado el nivel de spam que recibe en su cuenta de correo? ¿Ha detectado intentos de acceso a su cuenta en determinado servicio? Entonces, chequee si sus datos aparecen en algún *leak* de los que recopila Have I been pwned?[2]. Dependiendo de los resultados de su búsqueda en ese servicio, actúe cambiando contraseñas, activando dobles factores de autenticación, y plantéese si no merece la pena cambiar de número de teléfono.

Los 'malos de verdad' tienen, además, la posibilidad de adquirir, a precios interesantes, información de multitud de registros públicos que hayan sido vulnerados (registros de propiedad, padrones de impuestos, registros mercantiles, documentos privados, etc.). Todo lo necesario para preparar un ataque de Ingeniería Social a su persona, empresa o administración con las mayores garantías de éxito posible. Y un ejemplo claro es la utilización que ya se ha demostrado en España de la información de la Plataforma de Contratación del Sector Público, donde las administraciones publican sus licitaciones, y en las que se vierte información que puede ser de mucho interés para los delincuentes: nombres y cargos de personal técnico de la administración, direcciones de correo electrónico y postal, empresas o profesionales adjudicatarios de contratos, importes de las adjudicaciones, formas de facturación, etc. Y es obligatorio hacer esas publicaciones, lo mismo que ocurre con los portales de transparencia de las diferentes administraciones, donde también hay información que puede usarse, lamentablemente, para tratar de obtener un beneficio ilícito.

Para terminar, quiero plantear al lector unas reflexiones: ¿De verdad es necesario exponerse tanto en los medios sociales? ¿No será más priudente pensar mejor qué publicamos sobre nuestra vida privada? ¿No se puede procedimentar mejor qué información publican las Administraciones Públicas sobre sí mismas, los datos que manejan, y sus relaciones?
Quizá nos haga falta más sentido común para estar a gusto con la tecnología y ponérselo más difícil a los ciberdelincuentes.

Referencias

[1] https://pleaserobme.com/
[2] https://haveibeenpwned.com/
[3] https://contrataciondelestado.es/wps/portal/plataforma

MGEIT®

eGob®

COBIT® 2019 + ISO 38500
IT Governance
Gobierno TI

CERTIFÍCATE EN
GOBIERNO DE TI

Gobierno de Información y Tecnología EGIT es un nivel de madurez sobre la Gestión de las Tecnologías de la Información ITSM que consigue Alinear la Tecnología al Negocio y no viceversa. Puede haber Gestión sin Gobierno, pero jamás habrá Gobierno sin Gestión. Y tú ¿Gobiernas o solo Gestionas la Información y la Tecnología?

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones de 5 horas en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Curso de Doble Certificación del Master de Gobierno y Gestión de Información y Tecnología MasterGEIT®

CONVOCATORIAS 2022/23

- **ABRIL 2023 (Formato Martes y Jueves Tardes)**
  Martes 4, jueves 6, martes 11 y jueves 13
- **MAYO 2023 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 5, sabado 6, viernes 12 y sábado 13

eGob®

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es

El Plan Nacional de Ciberseguridad

A finales del mes de marzo, el Gobierno de España aprobó el Plan Nacional de Ciberseguridad, que desarrolla la Estrategia Nacional de Ciberseguridad de 2019, con una importante dotación económica, de alrededor de 1.000 millones de euros para los próximos tres años. Una iniciativa así, y con una inversión de este calibre, merece la pena ser analizada por Tecnología y Sentido Común.

Es de todos conocidos que la seguridad cuesta dinero y esfuerzo, y a estas alturas también debería saber todo hijo de vecino que, aunque la inversión económica es un factor muy importante en la implementación de las medidas de seguridad, no garantiza el completo éxito de las mismas, por elevada que aquella sea.

El pasado 29 de marzo de 2022, el Consejo de Ministros del Gobierno de España aprobó el Plan Nacional de Ciberseguridad [1], que según la nota de prensa distribuida a los medios, está dotado de alrededor de 1.000 millones de € para acometer más de 150 iniciativas diferentes en este ámbito de la Ciberseguridad. Este Plan se define para desarrollar la Estrategia Nacional de Ciberseguridad, que, aprobada en 2019, al parecer había tenido poco recorrido hasta el momento.

La aprobación de este Plan coincide en el tiempo, y no es una mera casualidad, con la aprobación de las medidas especiales que el Gobierno ha tomado para afrontar las consecuencias de la guerra causada por la invasión rusa de Ucrania. Hay que tener en cuenta que una buena parte de los grupos de ciberdelincuentes que operaban en los países occidentales estaban radicados en Rusia, e incluso en algunos casos protegidos o esponsorizados por el propio gobierno ruso, de acuerdo a las informaciones que manejan los servicios de seguridad europeos y estadounidenses. De hecho, el propio presidente de los EEUU, Joe Biden, advirtió abiertamente a Rusia, en julio de 2021 [2], de las consecuencias que tendría que ese país siguiera permitiendo operar a estos grupos desde su territorio, con total impunidad, contra empresas e intereses norteamericanos.

CONTINÚA EN PRÓXIMA PÁGINA

Aunque la información detallada del Plan aún no se conoce, sí se han destacado del mismo una serie de iniciativas:

• La creación de la plataforma nacional de notificación y seguimiento de ciberincidentes y de amenazas que permita intercambiar información, en tiempo real, entre organismos públicos y privados.

• Impulsar la puesta en marcha del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos.

• El desarrollo de un sistema integrado de indicadores de ciberseguridad a nivel nacional.

• Incrementar la creación de infraestructuras de ciberseguridad en las comunidades y ciudades autónomas y las entidades locales.

• Impulsar la ciberseguridad de pymes, micropymes y autónomos.

• Promover un mayor nivel de cultura de ciberseguridad.

A la espera de ver en qué se concreta exactamente el Plan y cuáles son esas 150 iniciativas que contiene, es conveniente resaltar que:

• Desarrollar un Plan así no es fácil ni barato, y es de alabar que el Gobierno de España haya tomado cartas en el asunto. El Departamento de Seguridad Nacional, dependiente de la Presidencia del Gobierno estará al cargo de su coordinación, e imaginamos que algunas de esas iniciativas no se harán públicas por motivos de seguridad.

• Sin embargo, con una Estrategia Nacional de Ciberseguridad aprobada en 2019, tardar más de dos años en redactar un Plan para llevarla a cabo, y que haya tenido que ser una guerra la que haya acelerado su aprobación, no son señales precisamente de tomarse el problema demasiado en serio desde el ámbito político. Vaya por delante que los grandes profesionales de la seguridad que tiene el Estado habrán hecho todo lo posible para que este Plan saliera adelante lo antes posible.

• Ha habido en los últimos tiempos incidentes graves de ciberseguridad en ministerios españoles, como los sufridos por el Ministerio de Trabajo, y ni siquiera entonces se aceleró la aprobación de este Plan, o al menos, no ha trascendido.

• Alguna de estas iniciativas del Plan ya está en marcha, como el Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos, que aunque no está funcionando a pleno rendimiento, ya hace unos meses que se licitó por vía de urgencia por el Ministerio de Economía [3], por una importante cantidad de dinero.

El resto de iniciativas que han trascendido públicamente tienen mucha lógica, y deben apuntar hacia quienes más difícil lo tienen para implantar una adecuada ciberseguridad por sus propios medios: PYMES, administraciones locales y ciudadanos, fundamentalmente. Son colectivos muy vulnerables a los ciberataques y estafas on line, que pueden dañar la economía del país, y por tanto, es importante que se realicen iniciativas específicas y de amplia difusión.

Otro aspecto donde el Plan deberá poner énfasis es en el de la protección de las infraestructura críticas, que ya cuenta con una legislación específica, pero que deberá ser reforzada su aplicación. De hecho, al día siguiente de aprobar el Plan Nacional de Ciberseguridad, el Gobierno aprobó un real decreto-ley de seguridad en las comunicaciones 5G, que establece las medidas de seguridad que ha de cumplir el despliegue de esa red de comunicaciones por parte de las compañías operadoras licenciadas por el Gobierno.

No hay duda de que se ha iniciado un camino, y que éste debe ser recorrido con una adecuada dirección, la dotación presupuestaria adecuada, y la firmeza necesaria para que se cumpla lo previsto. Y en ese camino los profesionales de las TIC y de la ciberseguridad debemos aportar nuestro granito de arena, aunque sea desde la concienciación de nuestros allegados.

La ciberseguridad es cosa de todos. Responsabilicémonos.

Referencias

[1]https://www.ccn-cert.cni.es/seguridad-al-dia/actualidad-ccn/11667-aprobado-el-plan-nacional-de-ciberseguridad.html
[2] https://www.france24.com/es/ee-uu-y-canad%C3%A1/20210710-estadosunidos-rusia-biden-ciberataques-putin
[3]https://www.lainformacion.com/empresas/calvino-adjudica-telefonica-indra-centro-ciberseguridad/2859405/

DAMA + ISO 38505
Data Governance
Gobierno del Dato

CERTIFÍCATE EN
GOBIERNO DEL DATO

Los datos confiables se han convertido en la materia prima imprescindible de la toma de decisiones estratégicas en la Era Digital tanto en Administracion Publica como Empreasas Privadas. La multitud de dispositivos, fuentes y naturalezas del dato obliga a un adecuado Gobierno y Gestión del Dato. Si lo tuyo es tomar decisiones certificate en Data Governance.

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Mas información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones de 5 horas en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Curso de Doble Certificación del Master de Gobierno y Gestión de Información y Tecnología MasterGEIT®

CONVOCATORIAS 2022/23

- **MAYO 2023 (Formato Martes y Jueves Tardes)**
  Martes 2, jueves 4, martes 9 y jueves 11
- **JUNIO 2023 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 2, sabado 3, viernes 9 y sábado 10

eGob®
Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es

Consejos de Ciberseguridad (I)

Desde muchos ámbitos se nos habla de ciberseguridad. Desde esta colaboración mensual en Tecnología y Sentido Común también lo hacemos. Sin embargo, poco se habla de qué debemos hacer para mantener un nivel de ciberseguridad aceptable en nuestros dispositivos. Como no queremos ser de aquellos que hacen eso de 'consejos vendo, que para mí no tengo', nos ponemos manos a la obra con dos artículos sobre el tema, para cerrar esta Séptima Temporada de TySC.

En las organizaciones de un cierto tamaño, el personal de Sistemas o de Seguridad de la Información realiza (o debería realizar) una labor técnica y pedagógica para que el personal que usa los recursos tecnológicos de esa organización esté razonablemente seguro en dicho uso, por la vía del establecimiento de medidas de protección y controles técnicos y organizativos, pero también por la vía de la formación y concienciación del factor humano de la ecuación de la seguridad.

Pero en organizaciones que no cuentan con esos recursos, o en el caso de los usos personales de las tecnologías de la información y las comunicaciones, se puede pensar en que no hay acciones que permitan que esos usos alcancen un nivel de ciberseguridad aceptable, de acuerdo a unos estándares mínimos. De esa sensación de que una parte importante de la 'población digital' se encuentra desprotegida y poco concienciada nacen las iniciativas públicas (y también privadas) para paliar la situación. Entidades como el Instituto Nacional de Ciberseguridad, a través de su Oficina de Seguridad del Internauta[1], o el CSIRTCV, el centro de ciberseguridad de la Comunidad Valenciana[2], tienen programas específicos de ayuda, concienciación y formación para sectores específicos de la población, tales como PYMES, jóvenes y personas mayores.

Sin embargo, en los últimos meses ya me ha sucedido varias veces que, en eventos públicos o en conversaciones privadas, personas recientemente preocupadas por la cuestión de la ciberseguridad (probablemente, a raíz de los ciberataques rusos asociados a la invasión de Ucrania) me han pedido consejos 'entendibles' para tratar de mejorar la ciberseguridad en sus dispositivos. Tras reflexionar sobre el tema, me he decidido a volcar esos consejos en artículos para Tecnología y Sentido Común, de manera que estén disponibles por si a otras personas les puedan resultar útiles. Algunos de los consejos pueden servir únicamente para terminales móviles. Otros, sólo para ordenadores portátiles o de sobremesa. Pero también hay consejos a aplicar válidos para cualquier dispositivo.

Consejo 1: La ciberseguridad es un proceso, es evolutiva, y no existe al 100%. No se pare, avance siempre.

Si se parte de una situación en la que no hay ninguna seguridad de la información en un determinado dispositivo, es evidente que cada medida correcta que se implemente irá incrementando el nivel de seguridad disponible, siempre que una medida no sea contraproducente para otra. El nivel de seguridad va evolucionando en dos líneas opuestas: los usuarios, fabricantes y expertos van implantando medidas de seguridad, y las aplicaciones y sistemas van siendo actualizados o implantados, generando nuevas oportunidades para aquellos que buscan cómo aprovechar sus vulnerabilidades para violentarlas.

CONTINÚA EN PRÓXIMA PÁGINA

Se ha de ser consciente que lo que supone un nivel de seguridad X hoy, sin hacer cambios de ningún tipo, dentro de un tiempo será un nivel de seguridad menor, simplemente por el hecho de que los ciberdelincuentes pueden haber encontrado nuevas grietas en el sistema. Es una especie de inflación del riesgo. Por ello, no podemos quedarnos parados en la implantación de determinadas medidas de seguridad, sino que debemos considerar la mejora de la seguridad un proceso continuo.

Consejo 2: Genere y almacene sólo la información digital estrictamente necesaria.

Gobiernos, corporaciones y ciberdelincuentes aprovechan nuestros datos para todo tipo de actividades y por diferentes motivaciones. Nuestra privacidad está en jaque desde que comenzamos a utilizar un terminal móvil. Y no sólo si nos lo roban. Las aplicaciones y sistemas operativos transfieren información a diferentes empresas sobre nuestros hábitos y actividades, ayudándolas a segmentarnos poblacionalmente para ser *targets* publicitarios más ajustados para diferentes campañas. Algunos países utilizan estos dispositivos como mecanismos de vigilancia masiva e, incluso, de control social. Y toda esa información puede llegar a caer en malas manos, si alguna de esas compañías sufre una brecha de seguridad, o simplemente, se es absolutamente inconsciente de lo que se está haciendo. Por tanto, toda información digital que no se genere no puede ser aprovechada por nadie en nuestra contra o en su favor.

A este respecto, más concretamente:

•No envíe copia digitalizada de sus documentos de identidad a nadie, bajo ningún concepto.
•Reduzca al máximo la información personal que proporciona en medios digitales.
•No publique su ubicación en redes sociales, ya que ello puede hacerle/a candidato/a a sufrir ciertos delitos contra la propiedad.

Consejo 3: La copias de seguridad son imprescindibles[3]

No importa si se está usando un PC, un smartphone, una tablet o una tostadora inteligente: hay que hacer copias de seguridad de los datos que contenga y de su configuración, si es posible. Evidentemente, para este consejo presuponemos que los datos que contiene el dispositivo que utilizamos son de algún valor para nosotros. En ese caso, no nos vendrá nada bien perderlos, en caso de avería, rotura, pérdida o sustracción del dispositivo, o en caso de que nos veamos afectados por un ramsomware.

En muchos entornos, la información que se almacena y gestiona en los sistemas de información vale muchísimo más que los propios sistemas tecnológicos que la tratan. Por ello, es conveniente que elija qué aplicación, método y periodicidad se ajusta mejor en cada dispositivo para realizar copias de seguridad. A tener en cuenta:

•No deje las copias en el mismo dispositivo del que se hace copia.
•Trate de seguir el patrón 3-2-1: mantener al menos tres versiones de los datos (los datos en producción y dos copias de seguridad), en dos dispositivos diferentes (el almacenamiento de producción y un disco externo USB, por ejemplo), y una de las copias en una ubicación geográfica diferente (por ejemplo, en la nube).

No por clásica esta medida es menos efectiva. Sólo requiere que seamos conscientes de la información que gestionamos, dónde se almacena, y dónde puede mantenerse a salvo en caso de desastre.

El mes que viene, más consejos.

Referencias

[1] https://www.osi.es/es
[2] https://www.csirtcv.gva.es/
[3] https://www.osi.es/es/actualidad/blog/2021/01/20/protege-tu-movil-ios-y-android-con-5-consejos

MGEIT® MPPM®

eGob®

COSO + ISO 37000
Corporate Governance
Buen Gobierno Corporativo

CERTIFICATE EN
BUEN GOBIERNO

El Buen Gobierno significa que la toma de decisiones dentro de la organización se basa en el espíritu, la cultura, las normas, las prácticas, los comportamientos, las estructuras y los procesos de la organización. El Buen Gobierno crea y mantiene una organización con un propósito claro que ofrece valor a largo plazo.

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la materia, su entorno y ámbito de aplicación, sus roles y responsabilidades que les permita participar en las inicativas.

Nivel de Certificación Executive*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las Buenas Prácticas, Metodologías y Bases de Conocimiento aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Leader*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de las normas y Estándares ISO aplicables con el fin de dirigir o participar en equipos de implementación.

Nivel de Certificación Skilled*

Acredita directivos y profesionales con un adecuado nivel de conocimientos respecto de la elaboracion de documentos, informes, planes, herramientas y/o artefactos que les permitan la aplicación práctica de los conocimientos.

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificacion Business&Co.® y alineados con la Norma UNE-EN ISO/IEC 17024:2012 Evaluación de la Conformidad. Requisitos Generales para los Organismos que realizan Certificación de Personas. Más información: https://businessandcompany.com/certificacion-de-personas

MISION

Nuestra misión consiste en instituir una nueva clase directiva capaz de liderar con éxito las oportunidades que nos brinda la era digital.

FORMACIÓN BUSINESS CLASS

- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones de 5 horas en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias y anécdotas.
- Cursos de Doble Certificación convalidables por asignaturas de los Masters MasterGEIT® y/o MasterPPM®.

CONVOCATORIAS 2022/23

- **JUNIO 2023 (Formato Martes y Jueves Tardes)**
  Martes 20, jueves 12, martes 27 y jueves 29
- **JULIO 2023 (Formato Viernes Tardes y Sábados Mañanas)**
  Viernes 21, sabado 22, viernes 28 y sábado 29

eGob

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es

Consejos de Ciberseguridad (y II)

En el número del mes pasado de Tecnología y Sentido Común publicamos la primera parte de un artículo sobre consejos de ciberseguridad, con los tres primeros consejos. Para cerrar esta Séptima Temporada de TySC, este mes publicamos la segunda parte del artículo sobre este tema.

Consejo 4:
PROTEJA SUS CREDENCIALES Y LOS ACCESOS, PERO CÓMODAMENTE [1]

En realidad, este consejo es una agrupación de varios relacionados. Hay que proteger nuestra identidad para que nuestra información se mantenga confidencial. Para ello, los sistemas de información utilizan diferentes métodos de identificación y autenticación. En los terminales móviles, podemos usar un PIN, una contraseña alfanumérica, un patrón o identificación biométrica, por huella dactilar o reconocimiento facial, para autenticarnos. En los PC, podemos usar credenciales con contraseñas complejas. Si no sabe generarlas, o no sabe cuán compleja [2] es su contraseña, hay servicios que permiten realizar ambas tareas. No almacene sus credenciales de acceso a servicios de Internet en los navegadores, ya que éstos son vulnerables y podrían robárselas.

Cambie las credenciales de sus servicios en la nube periódicamente, y active en todos los que pueda los sistemas de autenticación de doble factor. No repita credenciales entre diferentes servicios, para evitar que puedan ser reutilizadas en el caso de que uno de sus servicios sea violentado por ciberdelincuentes. Para evitar tener que recordar todas esas credenciales, use un **gestor de contraseñas**, a ser posible, multiplataforma, para poder llevar el fichero de contraseñas en diferentes dispositivos. Busque la manera de sincronizar esos ficheros de contraseñas, e intente evitar los gestores de contraseñas en la nube, ya que si fueran violentados o los gestiona una entidad poco fiable, todas sus contraseñas quedarían expuestas.

Consejo 5:
MANTENGA TODO ACTUALIZADO

Otro consejo clásico, y no por ello menos importante. Hay que mantener actualizados nuestros dispositivos, su sistema operativo y las aplicaciones. Tenga en cuenta que la vía de entrada a nuestros sistemas en muchas ocasiones son las vulnerabilidades que presenta el software. Por ello, expertos en la materia y los fabricantes trabajan en detectar y corregir dichas vulnerabilidades, publicando nuevas versiones de los productos software que las parchean.

Por tanto, es muy aconsejable que actualicemos nuestros dispositivos y aplicaciones tan pronto como haya nuevas versiones del software instalado, y es imperativo que instalemos rápidamente cualquier actualización de seguridad. Hay que tener en cuenta que es el periodo entre que un fabricante publica un parche de seguridad y que todos los dispositivos que tenían esa versión del software ya están actualizados cuando se producen más efectos dañinos de la vulnerabilidad parcheada, ya que es el propio fabricante quien da la información de la misma al publicar la actualización. Por tanto, ese tiempo ha de ser el mínimo posible.

Consejo 6:
UTILICE EL CIFRADO CON SENTIDO COMÚN

Si se cifra un documento, un pen drive USB, o una unidad de disco, nadie que no conozca la contraseña de descifrado y el método con el que se cifró podrá acceder a esa información, lo cual nos garantiza un buen grado de confidencialidad. En contraposición, el proceso de cifrar/descifrar la información ralentiza nuestro trabajo, e incluso puede llegar a ser insalvable en el caso de que olvidemos la contraseña de cifrado o si el sistema con el que se cifró deja de estar disponible.

No cometa el error de cifrar los dispositivos en producción y luego mantener las copias de seguridad descifradas. Pero si cifra las copias de seguridad, algo imprescindible si las almacena en la nube, asegúrese de que el método o aplicación de descifrado la va a tener disponible en caso de desastre, y almacene la contraseña de cifrado de forma segura en un dispositivo diferente.

En resumen, cifre, pero con sentido común, y sólo aquella información o dispositivos que realmente lo merezcan.

Consejo 7:
DESACTIVE LAS CAPACIDADES DE CONECTIVIDAD QUE NO ESTÉ USANDO

¿Para qué lleva el Bluetooth o el NFC de su móvil activado, si no lo está usando? Si ha conectado el portátil por cable a la red, ¿por qué no desactiva el interfaz wifi? Cualquier dispositivo de comunicaciones de nuestro ordenador o smartphone es susceptible de ser utilizado como puerta de entrada al sistema, o para robarnos información personal o bancaria, ya que hoy en día llevamos en nuestros dispositivos hasta los medios de pago. Los que somos algo paranoicos incluso llevamos las tarjetas de crédito que funcionan sin contacto dentro de fundas que impiden que funcionen correctamente hasta que las sacamos de dichas fundas para hacer un pago.

CONTINÚA EN PRÓXIMA PÁGINA

Consejo 8:
Ojo con las redes wifi públicas

Las redes inalámbricas públicas de hoteles, restaurantes, aeropuertos, centros comerciales, etc., sobretodo si son gratuitas, pueden suponer una amenaza para nuestra seguridad. En primer lugar, porque es muy fácil crear un punto de acceso inalámbrico falso (conocido como 'rogue AP' en el argot), a través del cual hacer cursar el tráfico de las víctimas para analizarlo en busca de información valiosa para el atacante, como credenciales de acceso a servicios, documentos, correos electrónicos, etc. Si va a utilizar alguna de estas redes públicas asegúrese de que los servicios de Internet a los que se va a conectar cifren la comunicación, o mejor aún, use un servicio comercial de VPN (red privada virtual), que se encargará de cifrar su tráfico desde su dispositivo hasta el terminador de túneles de la red, protegiendo así su información privada.
Si se decide por contratar uno de estos servicios de VPN, tenga cuidado en su elección, ya que también los hay fraudulentos. Con el servicio contratado, quizá hasta le interese usarlo cuando está haciendo uso de los servicios de banda ancha móvil de su operador de telefonía, ya que así mantendrá un mayor nivel de privacidad en su conexión.
Y si ya no va a conectarse más a una de esas redes wifi públicas, bórrela de su dispositivo.

Consejo 9:
Instale y configure correctamente un antivirus y un cortafuegos en su dispositivo

El uso de antivirus (ahora englobados en el concepto de EDR, End Point Detection and Response) se viene recomendando desde hace mucho tiempo, y raro es el PC que no dispone de uno. Sin embargo, aún hay mucha gente que se resiste a instalarse uno en el smartphone. Hágalo, no lo dude. Igualmente, es recomendable disponer de un servicio de cortafuegos (firewall) personal en nuestros dispositivos, que sea capaz de bloquear tráfico indeseado desde o hacia nuestro terminal. Los hay bastante simples de configurar, por lo que esa dificultad ya no es excusa para no usarlos en nuestros dispositivos móviles. En el PC, la mayoría de EDRs ya incorporan funcionalidades parecidas a las de un firewall, y el propio Windows lleva desde hace tiempo su servicio de cortafuegos, aunque no tanto como Linux.

Espero que sigamos juntos en la 8ª temporada de TYSC. ¡Tengan Uds. un feliz verano ciberseguro!

Referencias
[1] https://www.osi.es/es/actualidad/blog/2021/01/20/protege-tu-movil-ios-y-android-con-5-consejos
[2] https://howsecureismypassword.net/

IFEMA MADRID

Llámalo ingenio.
Llámalo IFEMA MADRID

Porque unimos talento, creatividad e imaginación.
Y las ideas inspiran nuevas ideas
y soluciones innovadoras. IFEMA MADRID.
Y ahora tú, vive la experiencia.

ifema.es

Siente la inspiración

NUEVOS MASTERS

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es