ESPECIAL

“Futuro y seguridad”

DE Tecnología & Sentido Común

ESPECIAL
AGOSTO
2023

Evento Cierre de temporada y Premio Tecnología y Sentido Común 2023 — 08

Asistentes digitales: Ángeles y Demonios — 14

El elefante en la habitación — 18

Respuesta a incidentes de seguridad (I — 22

Respuesta a incidentes de Seguridad (y II) — 26

¿Donde estarán mis datos? — 30

La criticidad de la cadena de suministro — 34

La hemos liado parda. ¿y ahora qué? — 38

¿Es un bulo? ¿Es un Deep Fake? Sí, Es Malinfo — 42

La (Ciber)seguridad de los vehículos conectados — 46

Cibercrimen,a la orden del día — 50

Ciberseguridad nacional: todos a una — 54

Lanzamiento del Service Management Institute SMI® — 58

ESPECIAL

Futuro y seguridad"

DE Tecnología & Sentido Común

EQUIPO TYSC
Javier Peris - El Gobernauta
Manuel D. Serrat - Futuro y Seguridad
Maryna Danylyuk - Economía de la Salud
Miguel Angel Arroyo - Hack & News
Juan Carlos Muria - Diario de una Tortuga Ninja
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Catalina Valencia - Ecosistema Emprendedor
Marcos Navarro - Ai Robot
Víctor Almonacid - La Nueva Administracion
Tommi Lattu - Nordic Mindset
Jesús López Peláz - Consejo de Amigo
Renato Aquilino - Marcos y Normas
Pablo Molina - Ethics Today
Marta Martín - Mentes Divergentes
Lucio Molina - América Próxima
André Pitkowsky - Meu Brasil

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

GABINETE JURÍDICO
Jesús López Peláz

ATENCIÓN AL LECTOR
soluciones@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://tecnologiaysentidocomun.com
soluciones@businessandcompany.com

(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.

MasterGEIT®
Gobierno y Gestión de Información y Tecnología

TITULACIÓN
MasterGEIT®

CONTENIDO DEL MASTER

Módulo 01: Gestión del Tiempo
Curso de Doble Certificación TSG4® Yellow Belt + TSG4® Green Belt

Módulo 02: Gestión de Procesos de Negocio
Curso de Doble Certificación BPM Executive + ISO 19510 Leader

Módulo 03: Dirección y Gestión de Proyectos
Curso de Doble Certificación OpenPM² (PjM) Executive + ISO 21502 Leader

Módulo 04: Dirección y Gestión de Programas
Curso de Doble Certificación OpenPM² (PgM) Executive + ISO 21503 Leader

Módulo 05: Gestión de Servicios de Tecnología
Curso de Doble Certificación FitSM Executive + ISO 2000 Leader

Módulo 06: Gestión de Seguridad de la Información
Curso de Doble Certificación CSX Executive + ISO 27000 Leader

Módulo 07: Gestión de la Continuidad del Negocio
Curso de Doble Certificación CBCI Executive + ISO 22301 Leader

Módulo 08: Gobierno de Información y Tecnología
Curso de Doble Certificación COBIT 2019 Executive + ISO 38500 Leader

Módulo 09: Gobierno del Dato
Curso de Doble Certificación DAMA Executive + ISO 38505 Leader

Módulo 10: Gobierno Corporativo
Curso de Doble Certificación COSO Executive + ISO 37000 Leader

*Niveles de Certificación pertenecientes a los Esquemas de la Entidad de Certificación 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

MISIÓN

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 del Master en Gobierno y Gestión de Información y Tecnología MasterGEIT®.

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

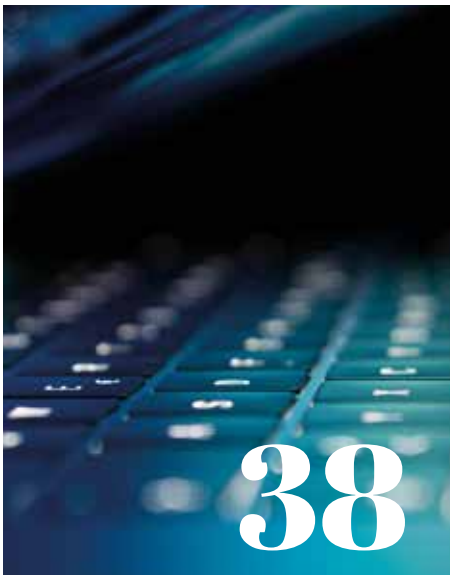
ESPECIAL
AGOSTO 2023

índice
DE CONTENIDOS

https://tecnologiaysentidocomun.com

08

Evento Cierre de temporada y Premio Tecnología y Sentido Común 2023


38

La hemos liado parda. ¿y ahora qué?

34

La criticidad de la cadena de suministro

54

Ciberseguridad nacional: todos a una

¡ic

#TYSC

Copyright 03

Índice de Contenidos 04

Evento Cierre de temporada y Premio Tecnología y Sentido Común 2023 08

Asistentes digitales: Ángeles y Demonios 14

El elefante en la habitación 18

Respuesta a incidentes de seguridad (I) 22

Respuesta a incidentes de Seguridad (y II) 26

¿Donde estarán mis datos? 30

La criticidad de la cadena de suministro 34

La hemos liado parda. ¿y ahora qué? 38

¿Es un bulo? ¿Es un Deep Fake? Sí, Es Malinfo 42

La (Ciber)seguridad de los vehículos conectados 46

Cibercrimen, a la orden del día 50

Ciberseguridad nacional: todos a una 54

Lanzamiento del Service Management Institute SMI® 58

Premios recibidos

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.

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

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.

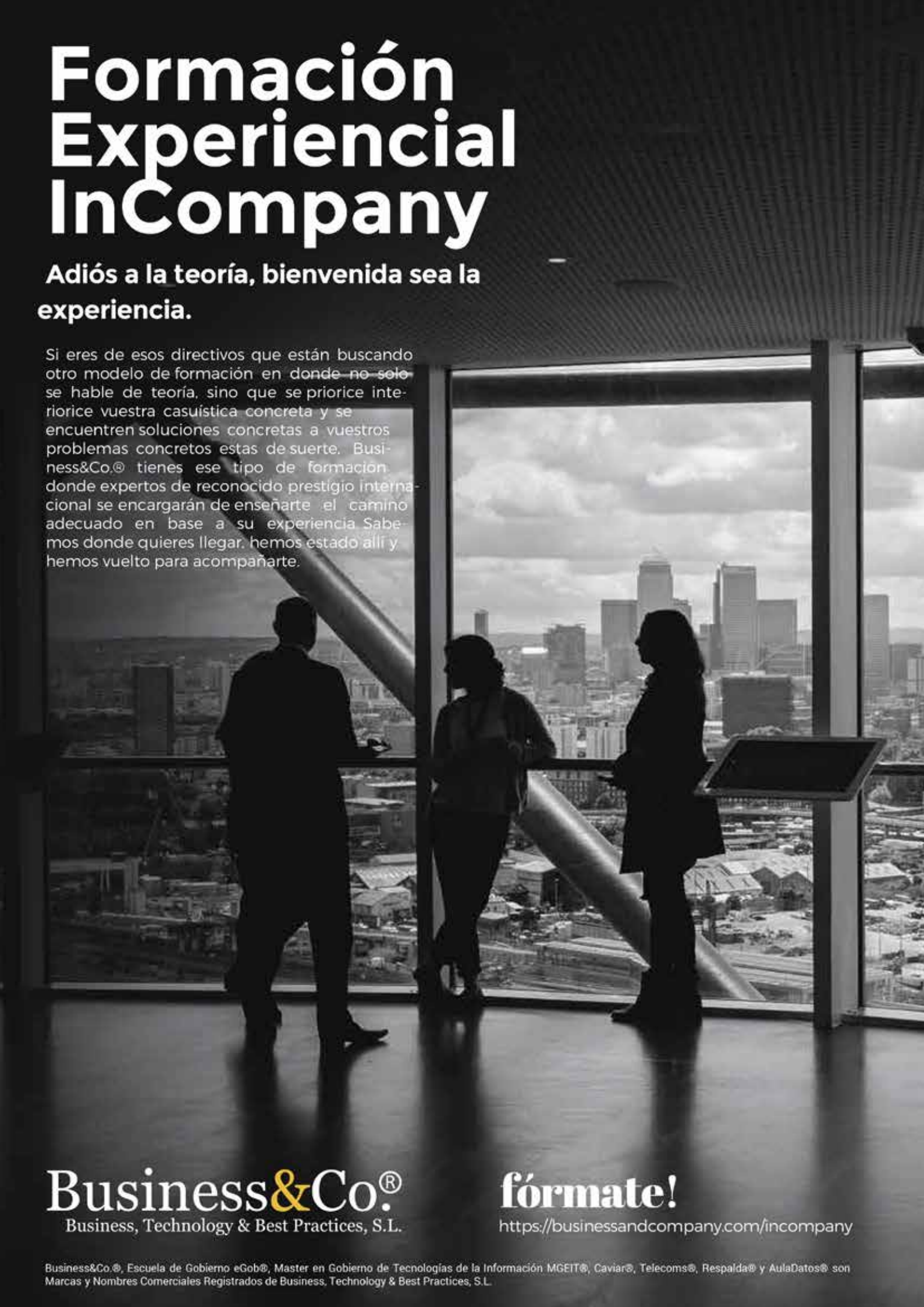
Premio 2022 ESET al Periodismo y Divulgación en Seguridad Informática

VI Premios ESET Periodismo y Divulgación: Tecnología y Sentido Común Premiada en la Categoría Blogs por el Articulo de Ricard Martínez "Seguridad en el Smartphone".
Los Premios ESET apuestan por la educación y la concienciación de la sociedad en materia de ciberseguridad, y los medios de comunicación son esenciales en este cometido.
Los periodistas y divulgadores son fundamentales para difundir el conocimiento necesario que permita a los usuarios disfrutar de la tecnología de una manera más segura.
Estos VI Premios ESET pretenden fomentar la divulgación de la ciberseguridad.

Formación Experiencial InCompany

Adiós a la teoría, bienvenida sea la experiencia.

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



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

fórmate!
https://businessandcompany.com/incompany

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.

Evento Cierre de temporada y Premio Tecnología y Sentido Común 2023

El miércoles 13 de julio se celebro en la sede de UNE Asociación Española de Normalizacion el evento de Clausura de la 2ª Temporada de Stakeholders.news la Revista Líder de la Alta Dirección y los Profesionales en Gobierno, Dirección y Gestión de Porfolios Programas y Proyectos donde se dieron cita importantes directivos tanto de la Administracion Publica como de empresas privadas.

El Acto fue presentado por Paloma Garcia Lopez, Directora de Normalización y Grupos de Interés de la Asociación Española de Normalización UNE y Javier Peris Chief Knowledge Officer CKO de Business&Co. y director de la revista Stakeholders.news quienes agradecieron al público la fantástica acogida a esta clausura.

Tras una presentación de UNE, su gran actividad de fomento, y difusión de la normalización y su la importante proyección internacional de la entidad a cargo de Paloma Garcia se dio paso a una ponencia magistral a cargo de Marc Berghmans Embajador del Centro de Excelencia PM² (CoEPM²) de la Comisión Europea sobre Gestion de Porfolios (Portfolio Management) y Gestión de Programas (Programme Management) con metodología PM2 de la Comisión Europea.

Recientemente el Centro de Excelencia PM² (CoEPM²) de la Comisión Europea amplio su alcance para desarrollar, mantener y promover metodologías adicionales que incluyen Gestión de Porfolios y Gestión de Programas.

Tras la ponencia de Marc Berghmans los miembros del equipo de Stakeholders.news presentes en el evento ofrecieron una Mesa Redonda moderada por Javier Peris donde explicaron el contenido más significativo de todos los artículos publicados durante esta temporada en cada una de sus respectivas secciones.

CONTINÚA EN PRÓXIMA PÁGINA

Mesa Redonda "Tecnología y Sentido Común"
Manuel Serrat
Sección
Futuro y
Juan Carlos Murra
Sección
Diario de una
Tortuga Ninja
Marcos
Navarro
Miguel Angel
Arroyo
Sección
Hack & News
Stakeholders

En primer lugar, Jose Luis Portela con la sección “Empleo y Futuro” hizo reflexionar al público sobre los importantes cambios de paradigma que van a producirse alrededor del empleo en las próximas décadas. Seguidamente Pedro Balsa, en la sección “Steering Committee” llevo a cabo importantes reflexiones sobre como valorar lo mejor poniendo como ejemplo el mundo del tenis profesional. Charo Fresneda desde su sección “El Lado Humano” puso como hace siempre a las personas en el centro poniendo el énfasis en una adecuada gestion de las emociones y la comunicación como factor determinante del logro de cualquier objetivo. Por su parte Juan Jesus Urbizu desde la sección “TecnoTransformación“ nos hizo ver que por encima de la tecnología están las personas que son las que deben poder usar y hacer valer esa tecnología y produzca los resultados adecuados que permitan obtener los beneficios esperados con los que alcanzar los objetivos estratégicos. Por su parte Juan Manuel Dominguez nos habló desde la sección “Organizaciones Resilientes” de importantes reflexiones relativas a la resiliencia.

Javier Peris moderador de la mesa agradeció a todo el equipo de la Revista, tanto a los presentes como a Angela Plaza, Carlos Pampliega, Ricardo Sastre y Luis Guardado quienes que no pudieron asistir al evento por compromisos profesionales.

Tras la Primera Mesa Redonda dedicada al equipo de la Revista Stakeholders.news se dio paso a una segunda Mesa Redonda donde participo el equipo de la Revista hermana “Tecnología y Sentido Común” la Revista Líder de habla hispana de la Alta Dirección y los Profesionales en Gestión de Proyectos, Gestión de Servicios, Gestión de Procesos, Gestión de Riesgos y por supuesto Gobierno de Tecnologías de la Información también moderada por Javier Peris Director de ambas publicaciones y en la que participaron cuatro miembros del equipo de la revista.
La Mesa comenzó con Manuel Serrat y la sección “Futuro y Seguridad” donde se puso el énfasis en la necesidad de una mayor concienciación de la debilidad tecnológica y la importancia de invertir esfuerzos y recursos ante la enorme amenaza que representa el crimen organizado. Juan Carlos Muria de la sección Diario de una Tortuga Ninja hablo de la importancia de unos adecuados procesos y formacion en el ámbito de la Gestion y el Gobierno de las Organizaciones y hablo de su ultimo articulo dedicado a la motivación, esa energía tremendamente poderosa. Marcos Navarro desde su sección “Ai Robot” dedicada a Robotic Process Automation RPA e Inteligencia artificial IA nos lanzo un mensaje claro de un presente en el que los humanos vamos a convivir con robots no necesariamente humanoides tanto en el ámbito profesional como en el personal a modo de asistentes para multitud de tareas. Por último, Miguel Angel Arroyo de la sección “Hack&News” puso el énfasis en la Ciberseguridad y en la Inteligencia de Amenazas y como la inteligencia artificial tambien puede ayudar de una manera considerable a reducir el impacto en las organizaciones respecto de la ciberdelincuencia.

Javier Peris hizo notar la gran densidad de conocimiento de la Revista Tecnología y Sentido Común con 16 colaboradores qe generan mensualmente un documento de más de cien páginas repletas de Tecnología pero sobre todo de sentido común convirtiendo esta publicación en la revista menos friqui de tecnología de las que existen hoy en el mercado y finalizo agradeciendo a Maryna Danylyuk de “Economía de la Salud”, Marlon Molina de “Es Tendencia, Ricard Martinez de ”Ojo Al Dato”, Catalina Valencia de “Ecosistema Emprendedor”, Victor Almonacid de “La Nueva Administracion, Tommi Lattu de “Nordic Mindset” Jesus Lopez Pelaz de “Consejo de Amigo”, Renato Aquilino de “Normas y Marcos”, Pablo Molina de “Ethics Today”, Marta Martín de “Mentes Divergentes” y Lucio Molina de “América Próxima” quienes con su trabajo y su absoluta generosa construyen mes a mes este impresionante documento que se puede disfrutar gratuitamente.

Siguiendo la agenda del evento, Javier Peris Director de ambas publicaciones invitó a participar a los nuevos fichajes de ambas revistas quienes explicaron ante la audiencia los contenidos que van a tratar dentro de cada una de sus respectivas secciones.

Los nuevos miembros del equipo que comenzarán a publicar en la próxima temporada que dará comienzo en setiembre son, por parte de Tecnologia y Sentido Común se incorporan Nacho Alamillo con la sección “Tecnoregulación en Prospectiva” quien nos traerá la actualidad reguladora tanto de España como de la Unión Europea en materia tecnológica con el foco en tecnologías disruptivas y basadas en cadena de bloques y entidad raíz de confianza. Y German Sanchis con la Sección “I’m IA” dedicada a la Inteligencia Artificial quien disculpó la asistencia al evento.

Por parte de la Revista Stakeholders.news se incorporan Jose Antonio Puentes, veterano Maestros y Director de Proyectos quien desde la sección “Tendiendo Puentes” se comprometió a compartir experiencias y consejos atesorados en su dilatada carrera profesional para que puedan

ser de utilidad al resto de profesionales y nuevas generaciones que se adentren en el maravilloso mundo del Cambio Organizacional. Luis Moran desde "Procesos y Personas" tambien ofreció todo su conocimiento alrededor de la Gestion de Procesos y Personas para ayudar al conjunto de la profesión desde su conocimiento y experiencia con el fin último de ayudar a crear mejores organizaciones. Para finalizar esta mesa redonda, Alejandro Aliaga desde "Radio Security" pondrá el acento mes a mes en desgranar nuevos vectores de amenazas que habitualmente pasan desapercibidos no por menos vulnerables y cuyos impactos en las organizaciones y en la vida de las personas pueden ser tremendamente significativos ¿Son los satélites vulnerables? nos anticipaba.
Llegado al punto álgido de la jornada se otorgaron los premios Tecnologia y Sentido Común 2023 y Stakeholders.news 2023" siendo entregados a UNE Asociación Española de Normalizacion y al Centro de Excelencia PM² (CoEPM²) de la Comisión Europea respectivamente.

Javier Peris, en nombre de todo el equipo de Tecnología y Sentido Común anunció como ganador del Premio "Tecnologia y Sentido Común 2023" a UNE Asociación Española de Normalizacion por su importante trabajo, su gran influencia y su elevada reputación mundial en el ámbito de la normalización, premio que fue recogido por Alfredo Berges, Presidente de UNE.

Alfredo Berges agradeció el Premio y elogio la labor de ambas publicaciones que se alienan con los objetivos de la asociación de crear un mundo mejor a través de la creación y difusión de Normas, Estándares, Metodologías y Bases de Conocimiento que permitan un futuro mejor. Alfredo Berges Presidente de UNE aseguró que "Es un reconocimiento que nos hace más ilusión si cabe al ser concedido por uno de nuestros miembros, Business&Co.®, Miembro Adherido Empresa de UNE, y que ha sido entregado por Javier Peris, quien preside el Comité de Gestión de servicios y Gobierno de la Tecnología de la Información y con el que tenemos una relación muy estrecha desde hace varios años".
Javier Peris, en nombre de todo el equipo de Stakeholders.news anuncio como ganador del premio "Stakeholders.news 2023" al Centro de Excelencia PM² (CoEPM²) de la Comisión Europea por haber ampliado su alcance para desarrollar, mantener y promover metodologías adicionales que incluyen Gestión de Porfolios y Gestión de Programas, premio que fue recogido por Marc Berghmans embajador de PM² de la Comisión Europea.

CONTINÚA EN PRÓXIMA PÁGINA

Marc Berghmans agradeció el premio y elogio la labor de difusión que viene llevando a cabo la revista no solo en el ámbito de Proyectos sino en el de Programas y Porfolios e invitó a la toda la audiencia a descargarse de manera gratuita y usar la metodología PM² que ha sido sufragada por todos los ciudadanos de la Unión Europea y ahora hay que aprovecharse de ello y usarla. Javier Peris le agradeció enormemente el esfuerzo que ha llevado a cabo Marc Berghmans con su presencia en el evento por encontrase en este momento de vacaciones.

Para finalizar el evento Javier Peris presentó a Antonio Galvez, Maestro Cortador de Jamón Ibérico quien realizaría una demostración de corete en vivo y degustación de un Jamon ibérico con el que deleitar el paladar de todos los asistentes e invito a todos a volvernos a leer la próxima temporada.

El Networking entre los asistentes, grandes profesionales tanto de la administración pública como de la empresa privada se extendió por mas de una hora y en donde además de degustar el Jamón Ibérico recién cortado por las manos expertas de un Maestro Cortador se pudieron compartir anécdotas, consejos y reflexiones entre todos los invitados.

Hace mucho tiempo que hablas.

¿Pero hace cuánto no dialogas?

Somos una organización global de beneficio para la comunidad cuya misión es crear normas para contribuir a la construcción de un mundo más seguro, sostenible y competitivo.

Creamos espacios de colaboración neutrales e inspiradores en los que compartir conocimiento para desarrollar, a través del diálogo y el consenso, normas que sirvan a los intereses de toda la sociedad y que movilicen a los que apuestan decididamente por la excelencia empresarial y la conciencia social.

UNE Normalización Española

Progreso compartido

une.org

Asistentes digitales: Ángeles y Demonios

Con la proliferación de los asistentes digitales, en nuestros smartphones o en dispositivos domésticos de sobremesa, se plantean sobre ellos cuestiones relativas a la privacidad y a la seguridad de esos elementos tecnológicos. Son productos en los que confluyen la Internet de las Cosas, la Inteligencia Artificial en la Nube, y la personalización o programabilidad de sus habilidades. Analicemos la cuestión en este primer artículo de la VII temporada de tecnología y Sentido Común.

Recientemente cayó en mis manos el último libro de la fenomenal periodista y divulgadora Mar Monsoriu, "Guía de Alexa para toda la familia", que leí con cierta prisa, pese a que no poseo ningún dispositivo de ese tipo. Me reconcomía la curiosidad de ver cómo, tras un importante periodo de documentación, la autora había conseguido reunir en una obra de este tipo información tan detallada sobre este tipo de altavoces inteligentes, el ecosistema de productos con los que se integra, su uso por parte de las diferentes 'edades' de los miembros de una familia, de personas con discapacidad, y de las ventajas de su utilización. Un trabajo concienzudo y detallado, además de útil, que recomiendo al lector si dispone de ese tipo de dispositivo o tiene pensado adquirir uno.

Durante tan amena lectura, sin embargo, y supongo que por deformación profesional, regresaron a mí las dudas sobre la seguridad y privacidad de este tipo de dispositivos y de los asistentes digitales en general. No me refiero específicamente a los dispositivos Alexa, sino también a los de otros fabricantes como Google, Samsung, Microsoft o Apple. No hay por qué negar que son muchísimas las personas que llevan activados los servicios del asistente digital de su terminal móvil. La voz de Siri de Apple es famosa, conocida incluso por quienes no usamos ni esa marca ni esa tecnología. El asistente de Microsoft, Cortana, o Bixby, el asistente de Samsung, junto con el asistente de Android o los dispositivos Google Nest/Dot y demás del ecosistema Google Home, no le van a la zaga al producto de Apple.

Sin embargo, hasta una obra tan utilitarista como el libro al que he hecho referencia anteriormente dedica un apartado a cuestiones de privacidad, ya que no se puede negar que este tipo de tecnologías forman parte ya de nuestro círculo más íntimo, nuestro hogar, y en ese ámbito lo más valorado es nuestra privacidad y nuestra seguridad. En este tema, es obvio que se hace muy patente la manida dicotomía de la seguridad y privacidad, por un lado, frente a la comodidad y utilidad, por otro lado, y cada cual se decanta más por uno de los lados de la balanza, según sus conocimientos, preferencias y necesidades.

CONTINÚA EN PRÓXIMA PÁGINA

Abstrayéndonos de productos, marcas o tecnologías, sí que creo que es importante que el lector tenga claro qué significa dar entrada de ciertas tecnologías en su hogar, o qué impacto puede suponer mantener activado el asistente digital de su terminal móvil. Y para ello, empecemos por lo básico: el interfaz de manejo de esos elementos es la voz. ¿Y cómo se capta la voz? Con un micrófono. ¿Y qué hace un micrófono? Grabar lo que está a su alcance. ¿Y cuando lo hace? Pues como queremos que el asistente responda a nuestras necesidades, lo habitual es que el micrófono esté siempre a la escucha, aunque haya una palabra mágica que active los servicios del asistente digital. Por tanto, quizá haya alguien que aún no haya caído en la cuenta de que todo lo que se dice en el alcance de uno de estos dispositivos está siendo grabado y analizado por el mismo. Y no voy a entrar a comentar los dispositivos de este tipo que llevan cámara integrada.

La siguiente pregunta lógica sería, desde mi punto de vista, ¿qué pasa con esas grabaciones? Los diferentes fabricantes, conscientes de los riesgos de privacidad que conllevan esas grabaciones, taxativamente niegan que se almacenen en sus sistemas, o que se haga con ellas nada más que analizarlas para dar cumplimiento a las órdenes del usuario, para ser eliminadas de inmediato. Sin embargo, varios han sido los casos[2] en que se ha podido demostrar que dichas grabaciones acaban siendo almacenadas en la nube de los diferentes fabricantes, bien por errores de programación, bien con el pretexto de mejorar la calidad del reconocimiento vocal del producto. Y por supuesto, que las grabaciones también se están utilizando para segmentar la publicidad que vemos en los diferentes dispositivos tecnológicos, porque cualquier pregunta sobre productos o servicios a uno de estos elementos acaba generando que nuestro navegador de Internet se inunde de publicidad sobre el tema. Y a veces, sin siquiera haberle preguntado específicamente al asistente, simplemente con una conversación doméstica. Por tanto, y pese a los ajustes de privacidad de los dispositivos, es innegable que su uso presenta un problema de privacidad evidente, que cada usuario debe ponderar frente a los beneficios que le reporta.

Por lo que a ciberseguridad se refiere, son productos muy acoplados a los servicios en la nube de los diferentes fabricantes, por lo que su software se actualiza con cierta periodicidad, y que las funciones que se pueden realizar con ellos, aunque impresionantes tecnológicamente hablando, no son especialmente críticas. Pero un dispositivo de esta tipología está continuamente conectado a Internet, por lo que si uno de ellos, o todos, fuesen violentados por grupos de delincuencia electrónica, sería una interesante fuente de información sobre los horarios, costumbres, nivel de vida, datos de identificación, etc. de sus usuarios. Y precisamente porque están pensados para un uso muy cómodo, los ajustes de seguridad que se pueden aplicar a estos elementos son, en la práctica, inexistentes. El usuario ha de confiar ciegamente en el fabricante, por lo que a la seguridad y actualizaciones del dispositivo se refiere. Sin embargo, es obvio que ningún dispositivo es imposible de *hackear*[3], y que para conseguirlo sólo hay que tener la motivación necesaria para hacerlo, y que merezca la pena el riesgo. De nuevo, no entraremos en las posibilidades que las grabaciones queden a disposición de ciberdelincuentes si los sistemas del proveedor del servicio son vulnerados.

Valorar los riesgos para la privacidad y seguridad de nuestro hogar debería ser uno de los elementos a tener en cuenta antes de adquirir dispositivos inteligentes para el mismo. Toda la domótica, si está conectada a Internet, es en sí misma una fuente de riesgo, ya que forma parte del universo de la Internet de las Cosas (IoT), del que ya hemos hablado en esta publicación[4]. Por tanto, **es crítico conseguir un equilibrio** entre nuestra seguridad y privacidad en el hogar, y los supuestos beneficios que este tipo de elementos, analizando con frialdad la cuestión y no dejándose llevar, simplemente, por el afán consumista o la incitación publicitaria.

REFERENCIAS

[1] Guia de Alexa para toda la familia. Mar Monsoriu Flor. Creaciones Copyright, S.L. ISBN 978-84-15270-53-9
[2]https://www.elespanol.com/omicrono/software/20200813/alexa-dejo-libre-grabaciones-usuarios-agujero-seguridad/512699500_0.html
[3] https://futurism.com/the-byte/eight-ways-hack-nest-camera
[4] El Tsumai IoT. TYSC Febrero 2021. Páginas 12-14. https://tecnologiaysentidocomun.com/ipages/flipbook/revista-tysc05-febrero-2021

MasterPPM®

Gobierno, Dirección, Gestión y Ejecución de Porfolios, Programas y Proyectos

TITULACIÓN
MasterPPM®

CONTENIDO DEL MÁSTER

Módulo 01: Gestión del Tiempo
Curso de Doble Certificación TSG4® Yellow Belt + TSG4® Green Belt

Módulo 02: Gestión de Procesos de Negocio
Curso de Doble Certificación BPM Executive + ISO 19510 Leader

Módulo 03: Dirección y Gestión de Proyectos
Curso de Doble Certificación OpenPM² (PjM) Executive + ISO 21502 Leader

Módulo 04: Dirección y Gestión de Programas
Curso de Doble Certificación OpenPM² (PgM) Executive + ISO 21503 Leader

Módulo 05: Gestión de Servicios de Tecnología
Curso de Doble Certificación FitSM Executive + ISO 20000 Leader

Módulo 06: Gestión de Proyectos Ágiles
Curso de Doble Certificación OpenPM² (Ágil) Executive + KANBAN Leader

Módulo 07: Dirección y Gestión del Porfolio
Curso de Doble Certificación OpenPM² (PfM) Executive + ISO 21504 Leader

Módulo 08: Gobierno de Proyectos, Programas y Porfolios
Curso de Doble Certificación P3MGO® Executive + ISO 21505 Leader

Módulo 09: Gobierno de la Externalización
Curso de Doble Certificación SGF Executive + ISO 37500 Leader

Módulo 10: Gobierno Corporativo
Curso de Doble Certificación COSO Executive + ISO 37000 Leader

*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

MISIÓN

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 convalidable por asignatura del Master en Gobierno, Dirección, Gestión y Ejecución de Porfolios, Programas y Proyectos MasterPPM®.

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

El elefante en la habitación

En el artículo del pasado mes de Tecnología y Sentido Común analizamos el fenómeno de los asistentes digitales, desde el punto de vista de la falta de privacidad y seguridad que pueden suponer. Reflexionando más, estamos en una situación, como usuarios de diferentes tecnologías, en que ya no es sólo que prácticamente regalemos nuestra privacidad a cambio de determinados servicios, sino que datos de partes de nuestra vida que queremos mantener privados pueden estar siendo recogidos de forma subrepticia por diferentes actores. Y de ello tratamos en este artículo.

Seguro que a la persona que está leyendo este artículo ahora mismo la situación que voy a narrar le resultará familiar. Buscamos la ruta hacia un lugar al que queremos desplazarnos en nuestro teléfono móvil. Nuestra aplicación de mapas nos guía solícitamente hasta allí, disfrutamos del día de asueto, visitando algunos emplazamientos de interés, y comiendo en un restaurante estupendo. Finalmente, regresamos a nuestro domicilio sin mayores inconvenientes. Es muy probable que la aplicación de mapas, transcurridas unas horas, nos pregunte si queremos dar información a otros viajeros sobre los lugares que hemos visitado, o sobre el restaurante al que hemos ido, mediante reseñas que podrán ser consultadas por cualquier persona interesada, y que incluso podemos adjuntar alguna fotografía ilustrativa. Todo inocentísimo, ya que con nuestro afán colaborador estamos ayudando a personas que ni siquiera conocemos a saber si un lugar merece o no la pena, o si el menú de un restaurante es sabroso, a precio competitivo o si disponen de platos para personas celíacas. Yo mismo lo he hecho hace poco tiempo, a la vuelta de las vacaciones.

Es obvio que nuestra aplicación de mapas conoce nuestra ruta de ese día gracias al servicio de ubicación del teléfono móvil que activamos para que nos ayudase a llegar a nuestro destino, y por tanto, por dicho posicionamiento geográfico, conoce los lugares concretos que hemos visitado. Como no tenemos nada que ocultar, nos da igual que el servicio de mapas recopile esa información de ubicación, la correlacione con datos de empresas y lugares turísticos, y tenga la deferencia de preguntarnos qué nos han parecido.

CONTINÚA EN PRÓXIMA PÁGINA

Pero si esa recopilación se realiza de forma masiva, a muchos usuarios del producto, o si los inocentes usuarios de la aplicación de mapas proporcionan toda la información que se les pide sobre los lugares que visitan, se pueden producir curiosos perfilados, de manera que las compañías 'que todos conocemos' venden a las empresas para ajustar mejor sus targets publicitarios o, sencillamente, tratar de vendernos sus productos de forma directa (emails, mensajes, llamadas telefónicas, etc.).

Ése es el 'elefante en la habitación' del que nadie quiere hablar. O casi nadie, porque este comportamiento ya fue criticado por Richard M. Stallman, hacker y apóstol del software libre, en múltiples ocasiones, llegando a recomendar librarse del smartphone [1]. Todos sabemos que nos espían, que nos tienen perfilados en cuanto a nuestros hábitos de consumo, y que estas compañías saben más de nosotros que nosotros mismos. Y todo ello, a cambio de casi nada. Simplemente por disfrutar unos servicios que no existían hace relativamente poco tiempo pero que se nos han hecho imprescindibles. ¿Cómo viajábamos en coche antes de los navegadores GPS? Pues consultando un mapa antes de salir, y revisándolo si las cosas no iban bien durante la ruta. ¿Cómo encontrábamos un restaurante al que ir a cenar? Consultando las páginas amarillas o preguntando a algún amigo. Ninguna de esas actividades dejaba un rastro tan claro y permanente como actualmente. Y sobre todo, nadie hacía negocio con nuestra información personal, nuestros gustos y nuestras actividades diarias.

Sin duda, la recopilación de datos que hacen todas las aplicaciones que utilizamos está recogida en los acuerdos de licencia que todos aceptamos sin leer, y la normativa de protección de datos obliga a mantener un nivel de seguridad aceptable de esos datos y a no hacer tratamientos abusivos de los mismos. Sin embargo, según algunos investigadores en ciberseguridad, algunas aplicaciones, como TikTok, Instagram o Facebook están comenzando a realizar una práctica que, como mínimo, es discutible: cuando se clica en un enlace desde la aplicación, icho enlace se abre en un navegador interno de dicha aplicación, y toda la información que se intercambia con la web en la que reside el enlace es recogida también por la aplicación móvil, incluyendo contraseñas y números de tarjeta de crédito, por ejemplo [2]. De hecho, el funcionamiento de la aplicación de TikTok, que recordemos que es una compañía china, y por tanto, sujeta a los mandatos del gobierno de ese país, se considera tan grave en algunos ámbitos incluso la FCC norteamericana ha llegado a pedir a Google y Apple que la prohíban en sus markets de aplicaciones [3].

Es obvio que la FCC ve la paja en el ojo ajeno (chino, en este caso) pero no la viga en el propio, porque justamente Google basa todo su negocio en la recopilación de datos de usuarios para la segmentación publicitaria en múltiples formatos. Pero es obvio que para el gobierno USA, la popularidad de esta aplicación de origen chino es una clara

amenaza, por la información que está recopilando. Por situaciones similares, el ejército estadounidense prohibió a sus miembros el uso de aplicaciones de fitness cuando salían a correr porque del análisis de los datos que los propios militares publicaban se podían deducir las ubicaciones de bases militares secretas [4].

Parece ésta una guerra perdida, la de la privacidad en el siglo XXI, pero no por ello debemos dejar de ser precavidos y dejar de dar las batallas que corresponda y cuando corresponda en su defensa.

REFERENCIAS

[1]https://elpais.com/retina/2019/02/22/tendencias/1550819915_405396.html
[2]https://hipertextual.com/2022/08/tiktok-inserta-un-codigo-que-capta-hasta-tus-contrasenas-y-tarjetas-de-credito
[3]https://www.washingtonpost.com/business/2022/06/29/fcc-tiktok-ban-apple-google/
[4] https://www.bbc.com/mundo/noticias-42859883

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

Respuesta a incidentes de seguridad (I)

En todos los ámbitos de la seguridad, no sólo de la ciberseguridad, y como decía un proverbio chino "Hombre prevenido vale por dos". Por esa razón, y ante la eventualidad de un incidente, en esos diferentes ámbitos de la seguridad proliferan los planes, simulacros, entrenamientos y pruebas para verificar cómo responde la organización ante esas situaciones. Por supuesto, en ciberseguridad también hay que tener muy claro cómo debemos responder ante determinadas situaciones, porque si, cuando éstas se produzcan, se ha de pensar en qué se va a hacer, el desastre está servido, ya que se trata de situaciones estresantes y poco propensas a la toma de decisiones bien ponderadas. De ahí la necesidad de saber gestionar los incidentes y tener una adecuada planificación.

Seguro que todos nuestros lectores, de niños, en el colegio o instituto, han participado en algún simulacro de evacuación, en previsión de que se declarase un incendio u otra emergencia que la pudiese requerir. Probablemente, en su vida adulta, muchos de nuestros lectores españoles habrán participado en formación sobre el plan de autoprotección de su organización, e incluso, en algún simulacro de evacuación de su centro de trabajo. Todos los gobiernos nacionales disponen de planes de defensa militares ante diferentes amenazas externas, y muchos de ellos tienen planes de protección civil que se activan ante ciertas eventualidades industriales, de tráfico, climáticas o geológicas Como curiosidad, quizá la mayoría de nuestros lectores no sepan que algunos gobiernos disponen de planes (secretos) de respuesta ante situaciones que algunos considerarían descabelladas, tales como un contacto extraterrestre, por más que la ONU advirtiera de que no se disponía de un plan global frente a esta eventualidad [1].

Todos los ejemplos del párrafo anterior vienen a demostrar que, por lo que a la seguridad se refiere, constituye una necesidad imperiosa la existencia de planes y protocolos que cubran las diferentes eventualidades que pueden poner en riesgo la pervivencia de un determinado sistema. En esos planes y protocolos muy probablemente se incluyan los roles implicados en cada una de las eventualidades, la formación que hay que darle a los implicados, y quizá, los entrenamientos o simulacros que serán necesarios para comprobar la efectividad de los planes, los protocolos y la formación del personal.

Pues bien, la ciberseguridad no puede ser ajena a estas situaciones, y existen diferentes aspectos sobre los que actuar, como los planes de continuidad de negocio, los planes de recuperación ante desastres, o los **protocolos de gestión de ciberincidentes**. Y precisamente a éstos últimos vamos a dedicar en Tecnología y Sentido Común una pequeña serie de artículos, tratando de resumir o destilar las cuestiones básicas importantes, pensando en que cualquiera pueda utilizar esta información para iniciar el camino hacia una adecuada respuesta a este tipo de incidentes.

Obviamente, en esta temática no se parte de cero, y la información que contienen estos artículos está destilada a partir de dos documentos oficiales que considero fundamentales:

•ISO 27035:
Gestión de incidentes de seguridad de la información

•NIST SP 800-61:
Computer Security Incident Handling Guide

Asimismo, si el lector desea profundizar en este tema, puede aprovechar una obra con una visión más amplia, y basada en la experimentada experiencia práctica de la autora. Se trata del libro "Gestión de Incidentes de ciberseguridad" de Maite Moreno [2], en el que se desgranan con detalle los aspectos fundamentales de ambas normas y de los conceptos y consejos que se van a dar en esta serie de artículos.

CONTINÚA EN PRÓXIMA PÁGINA

Evidentemente, para responder a un ciberincidente, debemos contar con **capacidad** para ello, en el más amplio sentido de la palabra. Debemos desponer de personal o servicios capaces de detectar que se está produciendo, de clasificarlo, y de responder ante el mismo. También debemos contar con la capacidad para planificar la respuesta, mientras no estemos siendo atacados, y de realizar tests o simulacros de ataque para revisar dicha planificación y su adecuación a la realidad. Para incrementar nuestra capacidad de respuesta ante este tipo de incidentes, habitualmente se suele confiar en un Security Operations Centre (SOC), que a su vez debe contar con un CSIRT/CERT (Computer Security Incident Response Team/Computer Emergency Response Team), que será quien lidere, y/o sea el encargado de, muchas de las tareas relacionadas con la respuesta ante el incidente. Sin embargo, habrá otros roles en la organización que estarán implicados en los planes de respuesta, tales como la Alta Dirección, el personal informático o de comunicaciones, o incluso, el personal del departamento legal y de comunicación.

Un ciberincidente, según la NIST SP 800-61, tiene un ciclo de vida de cuatro fases:

1.Preparación
2.Detección y Análisis
3.Contención, Erradicación y Respuesta
4.Actividades Post-Incidente

A mi juicio, la etapa más importante es la de preparación, porque ***"todo lo que no es planificación es improvisación"***, en palabras del director de nuestra publicación, Javier Peris. ¿Se puede responder adecuadamente a un incidente sin estar preparados? Quizá sí, pero quizá el coste, el tiempo o los resultados finales no sean los adecuados. Por tanto, si enfocamos nuestro esfuerzo en pensar, elaborar, documentar, y mantener los protocolos de respuesta, y en preparar a la organización frente a los diferentes tipos de ciberincidentes planificados, cuando éstos se produzcan, o bien el tiempo necesario para detectarlos, contenerlos y responder se reducirá drásticamente, o bien se reducirá su impacto dañino. Y si tras el suceso, analizamos toda la información para obtener lecciones aprendidas que puedan mejorar los protocolos, miel sobre hojuelas.

Pero parte de la **fase de preparación** no sólo consiste en tener protocolizados los diferentes tipos de incidentes de seguridad que creamos conveniente. Hoy en día, es necesario monitorizar nuestros sistemas, ya que sin ello va a ser muy complicado detectar los algunos de los incidentes en sus etapas tempranas. Y también es necesario mantener una vigilancia sobre los diferentes indicadores de compromiso y las fuentes de información de ciberinteligencia u OSINT [3] para conocer en qué riesgos se puede ver involucrada nuestra organización, a través de conocer qué información nuestra está disponible en ciertos ámbitos.
Preparemonos frente a lo posible, para que cuando ocurra, no nos pille desprevenidos o sin saber qué hacer. Y preparémonos también frente a lo improbable, como lo eran ciertos 'cisnes negros', que han surgido en los últimos tiempos (COVID-19, volcán de La Palma, o invasión rusa de Ucrania).

En el segundo artículo de esta serie, nos centraremos en las fases de detección y respuesta frente al ciberincidente, así como en las actividades post-incidente.

REFERENCIAS

[1] https://news.un.org/es/story/2010/10/1202701
[2] Maite Moreno García. Gestión de Incidentes de ciberseguridad. 2022. Editorial RA-MA. ISBN 978-84-1897-173-0
[3] https://tecnologiaysentidocomun.com/ipages/flipbook/revista-tysc18-abril-2022 Páginas 12 a 14

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. 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 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®.

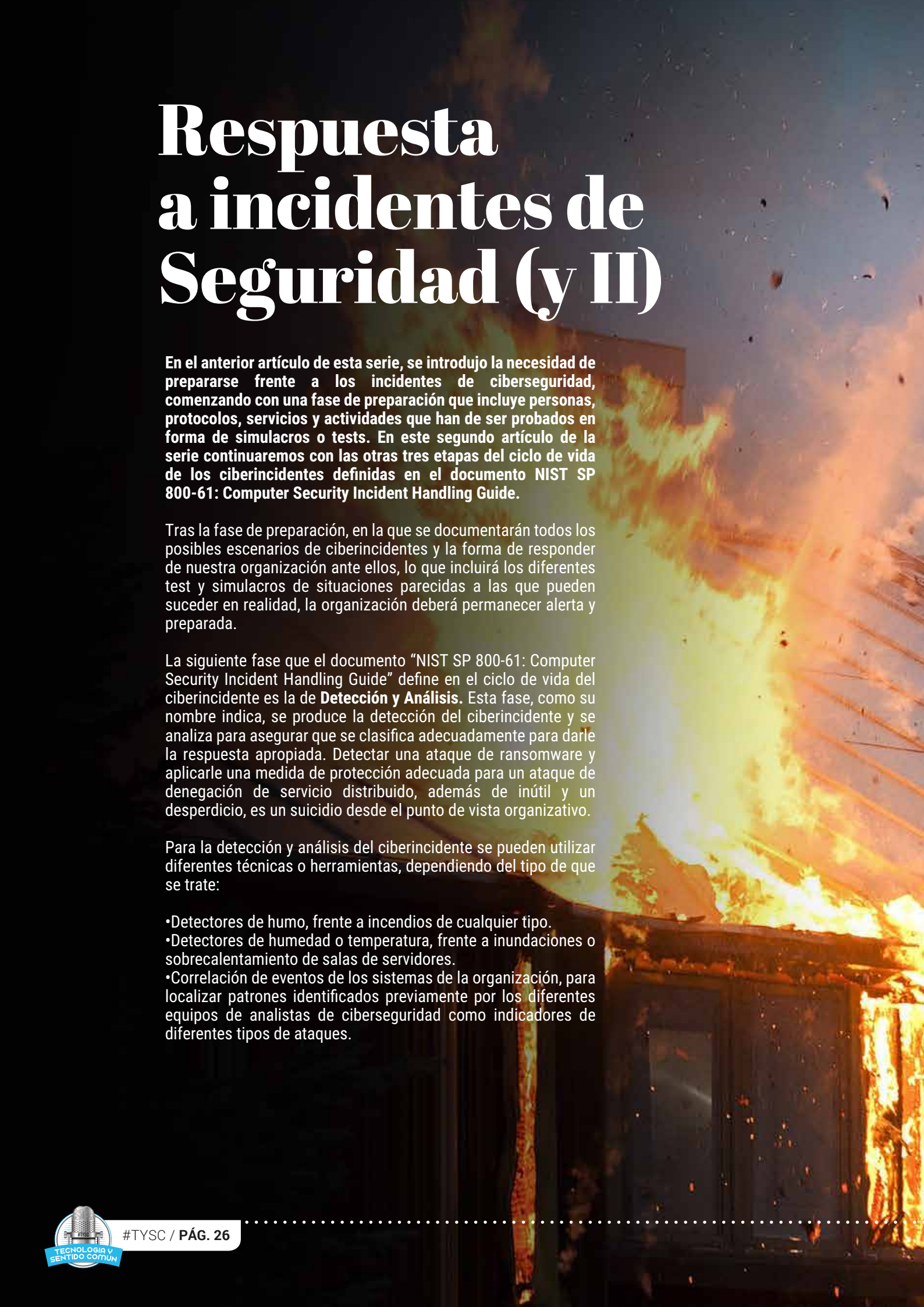
CONVOCATORIAS 2022/23

- **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

Respuesta a incidentes de Seguridad (y II)



En el anterior artículo de esta serie, se introdujo la necesidad de prepararse frente a los incidentes de ciberseguridad, comenzando con una fase de preparación que incluye personas, protocolos, servicios y actividades que han de ser probados en forma de simulacros o tests. En este segundo artículo de la serie continuaremos con las otras tres etapas del ciclo de vida de los ciberincidentes definidas en el documento NIST SP 800-61: Computer Security Incident Handling Guide.

Tras la fase de preparación, en la que se documentarán todos los posibles escenarios de ciberincidentes y la forma de responder de nuestra organización ante ellos, lo que incluirá los diferentes test y simulacros de situaciones parecidas a las que pueden suceder en realidad, la organización deberá permanecer alerta y preparada.

La siguiente fase que el documento "NIST SP 800-61: Computer Security Incident Handling Guide" define en el ciclo de vida del ciberincidente es la de **Detección y Análisis.** Esta fase, como su nombre indica, se produce la detección del ciberincidente y se analiza para asegurar que se clasifica adecuadamente para darle la respuesta apropiada. Detectar una ataque de ransomware y aplicarle una medida de protección adecuada para un ataque de denegación de servicio distribuido, además de inútil y un desperdicio, es un suicidio desde el punto de vista organizativo.

Para la detección y análisis del ciberincidente se pueden utilizar diferentes técnicas o herramientas, dependiendo del tipo de que se trate:

•Detectores de humo, frente a incendios de cualquier tipo.
•Detectores de humedad o temperatura, frente a inundaciones o sobrecalentamiento de salas de servidores.
•Correlación de eventos de los sistemas de la organización, para localizar patrones identificados previamente por los diferentes equipos de analistas de ciberseguridad como indicadores de diferentes tipos de ataques.

•Monitorización de los sistemas y del tráfico de las redes de la organización.
•Integración de la monitorización y la correlación en sistemas SIEM (Security Information and Event Management), que además proporcionan funciones 'extra' que van a ser muy útiles en fases posteriores.
•Servicios de analistas de seguridad integrados en los SOC (Security Operations Centre), que descartan falsos positivos, y operan y mantienen actualizadas las herramientas de detección y análisis con las que cuente la organización.

El ciberincidente se habrá registrado correctamente en los sistemas de gestión de la compañía, y toda la información recopilada por el equipo de respuesta se encontrará disponible allí para las siguietnes actividades o fases. La salida de esta fase es una adecuada identificación del incidente y la recomendación de qué protocolos de respuesta hay que aplicar en la fase siguiente. Dicha fase, según la NIST SP 800-61, es la de **Contención, Erradicación y Respuesta**.

CONTINÚA EN PRÓXIMA PÁGINA

La **contención** del incidente, igual que ocurre con un incendio forestal, consiste en aplicar las medidas establecidas en la planificación para que los daños que produzca el incidente ya no puedan aumentar. Hablamos de cualquier tipo de perjuicio, tal como cifrado de ficheros, exfiltración de información, destrucción de información o equipos, reputacionales, o intrusiones para control a largo plazo de los sistemas y redes de la organización, como las que ejecutan las Amenazas Persistentes Avanzadas (o APTs, de sus siglas en inglés).

La **erradicación** consistirá en eliminar la parte activa de la amenaza, sea ésta un incendio, una inundación, un virus, un troyano, una consola de acceso remoto no autorizada, o credenciales fraudulentas o sesiones abiertas en determinados servicios como resultado del incidente. A este respecto, es importante ser capaces de conocer todos aquellos sistemas comprometidos por la acción del atacante. Atacante que, por cierto, puede ser un sistema automatizado o un humano que reaccione ante las acciones del personal de seguridad de la organización. Se puede ver esta subfase como la primera en la que, tras su finalización, el equipo de respuesta a incidentes de la organización puede comenzar a respirar con menos estrés.

La **respuesta** al incidente, como siguiente subfase, puede ser de varios tipos, y dependerá de los diferentes enfoques disponibles. Por ejemplo, puede estar protocolizado que no se debe pagar un rescate ante un ataque de ransomware, sino que hay que denunciar judicialmente y pedir el apoyo de un CERT (Computer Emergency Response Team) de referencia. La respuesta, cuando el ataque se produce a ciertos sistemas de alto valor estratégico, puede incluso ser pasar al contraataque, dejando fuera de servicio los sistemas del atacante, o, en algunos casos (los menos, lamentablemente), la detención de los autores o instigadores del ataque. Es importante que los roles implicados en cada uno de los protocolos de respuesta a ciberincidentes conozcan el alcance y las consecuencias de las actividades que realicen, o de su omisión a realizarlas, ya que alguno de ellos puede acabar mal si se hace lo que no debe [1]. De ahí la importancia de que todas las actividades estén adecuadamente definidas, con los roles asociados para su ejecución, y la asignación de roles a personas internas o externas de la organización se mantenga actualizada. Se dio el caso de una empresa que no quiso pagar ante un ataque de ransomware, pese a las amenazas y a que no isponía de copias de seguridad adecuadas. Cuando los operadores del ransomware cumplieron su amenaza de exfiltrar toda la información de la compañía que habían cifrado y sustraido, dicha empresa sólo tuvo que descargarse su propia información y retomar su actividad, reforzando eso sí las medidas de seguridad. Pero este caso es como que nos toque la lotería, y no es significativo estadísticamente hablando, porque no disponer de copias de seguridad es, en sí mismo, una prueba de la inexistencia de planificación alguna ante incidentes de este tipo.

Finalmente, la NIST SP 800-61 establece como última fase del ciclo de vida de los ciberincidentes todas las **actividades post-incidente**. Entre estas actividades hay una de especial interés, sobre todo para nosotros, amantes de las **buenas prácticas**: las lecciones aprendidas del ciberincidente. En un briefing, el equipo de respuesta y los diferentes roles implicados en el ciberincidente extraen del análisis posterior del mismo las conclusiones oportunas, enfocándose en la **mejora continua** de los protocolos y del desempeño del equipo en la ejecución de todas las tareas. Cualquier lección aprendida que permita que mejoren los resultados de la organización ante futuros ataques similares es bienvenida, incorporada al protocolo, en su caso, y testeada en los simulacros posteriores planificados. Y si encima ese conocimiento destilado se comparte (con la prevenciones oportunas) con otros miembros de la comunidad global de ciberseguridad, aún mejor. Todo lo que sea ponérselo más difícil a los ciberdelincuentes de todo pelaje siempre será bienvenido.

Prepárense para afrontar los ciberataques. ¡La siguiente víctima podemos ser cualquiera de nosotros!

Referencias

[1]https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach

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

¿Donde estarán mis datos?

A estas alturas, todos conocemos ya el concepto de 'la Nube'. Sin embargo, pocos comprenden que, en realidad, la Nube no es más que un conjunto de equipos o servicios de tecnologías de la información, propiedad de otra organización, que se alquilan según un modelo comercial de "pago por uso". Pocos se preocupan de saber dónde están realmente sus datos cuando están "en la Nube", y menos aún son los que se conocen en qué condiciones se alojan los equipos de computación y almacenamiento que permiten operar a esa nube.

Si el lector cree que este artículo va a centrarse en la ubicación geográfica de los centros de proceso de datos, está parcialmente equivocado. Que los datos residan en USA, China o San Marino, en este artículo nos da igual. Para el ámbito de este escrito, los datos están, simplemente, en "la NubeTM". Ya sabemos (o deberíamos intuir) que "la NubeTM" no es más que un conjunto de centros de proceso de datos (CPD) de diferentes propietarios, que se comercializan en un formato de pago por uso flexible. Tampoco describiremos las ventajas e inconvenientes de este modelo de comercialización, sino que nos vamos a centrar en el modelo de costes de estos centros de proceso de datos, que hace que se hayan tomado curiosas iniciativas para hacerlos más rentables y sostenibles medioambientalmente.

Según algunas fuentes, los costes totales de un CPD son, aproximadamente, los siguientes:

- Electricidad y aire acondicionado: 26 %
- Proyecto, ingeniería y mano de obra de la instalación: 23 %
- Hardware, alimentación ininterrumpida y organización: 21%
- Espacio físico: 15 %
- Mantenimiento y comunicaciones: 15 %

Por tanto, cualquier iniciativa que reduzca los costes en cualquiera de los conceptos de gasto será bienvenida por los propietarios de los CPD en producción, sobretodo, porque varios de ellos crecen conforme crece el volumen de suscripción de la capacidad del centro. Y no podemos perder de vista que algunos de estos aspectos a tener en cuenta en la explotación de un CPD deben tratar de reducir su huella medioambiental.

Hay conceptos de coste en los que un propietario de CPD poco puede influir, como el hardware a adquirir. Sin embargo, hay apartados en los que iniciativas radicales pueden ser económica y medioambientalmente muy interesantes, aunque planteen retos logísticos interesantes. Es demasiado obvia la propuesta de llevar los CPD a países donde el espacio físico y la mano de obra puedan ser más baratos, pero habrá que tener en cuenta qué servicios se podrán prestar desde esos países a organizaciones europeas, con el Reglamento General de Protección de Datos en la mano.

CONTINÚA EN PRÓXIMA PÁGINA

Pero, si reducimos el consumo eléctrico, podemos ahorrar costes y la emisión de CO2 a la atmósfera. Por ello, disponer de CPD en lugares más fríos puede ser una opción. Y lugares más frçios no necesariamente signifique construirlos más cerca de los polos, sino que también pueden construirse a muchos metros de profundidad. Y si se aprovechan agujeros ya excavados, el coste de construcción se reduce. Imagino que, simplificando, ésa fue la deducción de los impulsores del Lefdal Mine Datacenter [1], en Noruega, que decidieron aprovechar **una antigua mina de carbón** para construir en su interior un CPD de 120.000 m². No es discutible que una mina en desuso es un lugar en el que el m² debía ser barato. En Noruega no hace calor, precisamente, y a determinada profundidad la temperatura es constante, por lo que durante buena parte del año basta con impulsar aire frio del medio ambiente para conseguir que el CPD se encuentre en condiciones óptimas de temperatura para operar. Y en aquellas salas en las que no sea necesario que haya personas trabajando, la iluminación puede mantenerse apagada, por lo que los costes de energía pueden reducirse a un 60% de los habituales en una instalación de ese tipo. El mismo ahorro se producirá en las emisiones de CO2, claro, lo cual lo hace medioambientalmente más sostenible.

En esa línea, algunas compañías han decidido explorar otras opciones. En este caso, Microsoft ha confirmado, merced a su Project Natick, que los **CPD sumergidos en el mar** también son una opción viable [2], por razones similares al CPD noruego de Lefdal. Fundamentalmente, por los ahorros energéticos producidos al mantener la temepratura del CPD dentro de los umbrales operativos correctos prácticamente de forma gratuita. Naturalmente, aquí el reto para su construcción y explotación adecuada es la propia dinámica marina: corrientes, temporales, corrosión, accidentes de pesca, etc. Pero cuando se perfeccione la técnica de construcción de los mismos, y se localicen los mejores lugares para llevarlos a cabo, esta opción de los CPD sumergidos en el mar (o en lagos o embalses) puede resultar muy interesante.

Pero no sólo en minas o bajo el agua se están planteando centros de proceso de datos. Recientemente nos sorprendía la noticia [3] de que la Unión Europea había licitado un estudio de viabilidad para los **centros de proceso de datos espaciales**. Obviamente, la viabilidad de esta opción residiría en dos cuestiones fundamentales:

•La posibilidad de generar energía suficiente en centrales eléctricas fotovoltaicas espaciales, que generaran la electricidad necesaria para estos centros de proceso de datos, junto con un sistema óptico de comunicaciones de banda ancha.
•La construcción, puesta en órbita y explotación de esos centros de proceso de datos espaciales debería generar menos impacto ambiental que mantenerlos en la Tierra.

A falta de las conclusiones del estudio de la UE, esta opción parece menos viable a simple vista, pero es obvio que para viajes espaciales de larga duración, las naves espaciales deberán disponer de un CPD a bordo, por lo que este estudio de la UE puede ayudar a la optimización energética de este tipo de infraestructuras.

Si este tipo de CPD llegan a ser viables, entonces nuestro datos ya no estarán en "la NubeTM", sino que, literalmente, ascenderán a los cielos.

Referencias

[1] https://www.lefdalmine.com/
2]https://news.microsoft.com/innovation-stories/project-natick-underwater-datacenter/
[3]https://www.datacenterdynamics.com/es/noticias/thales-alenia-space-gana-el-estudio-de-viabilidad-de-la-ue-para-los-centros-de-datos-espaciales-ascend/

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

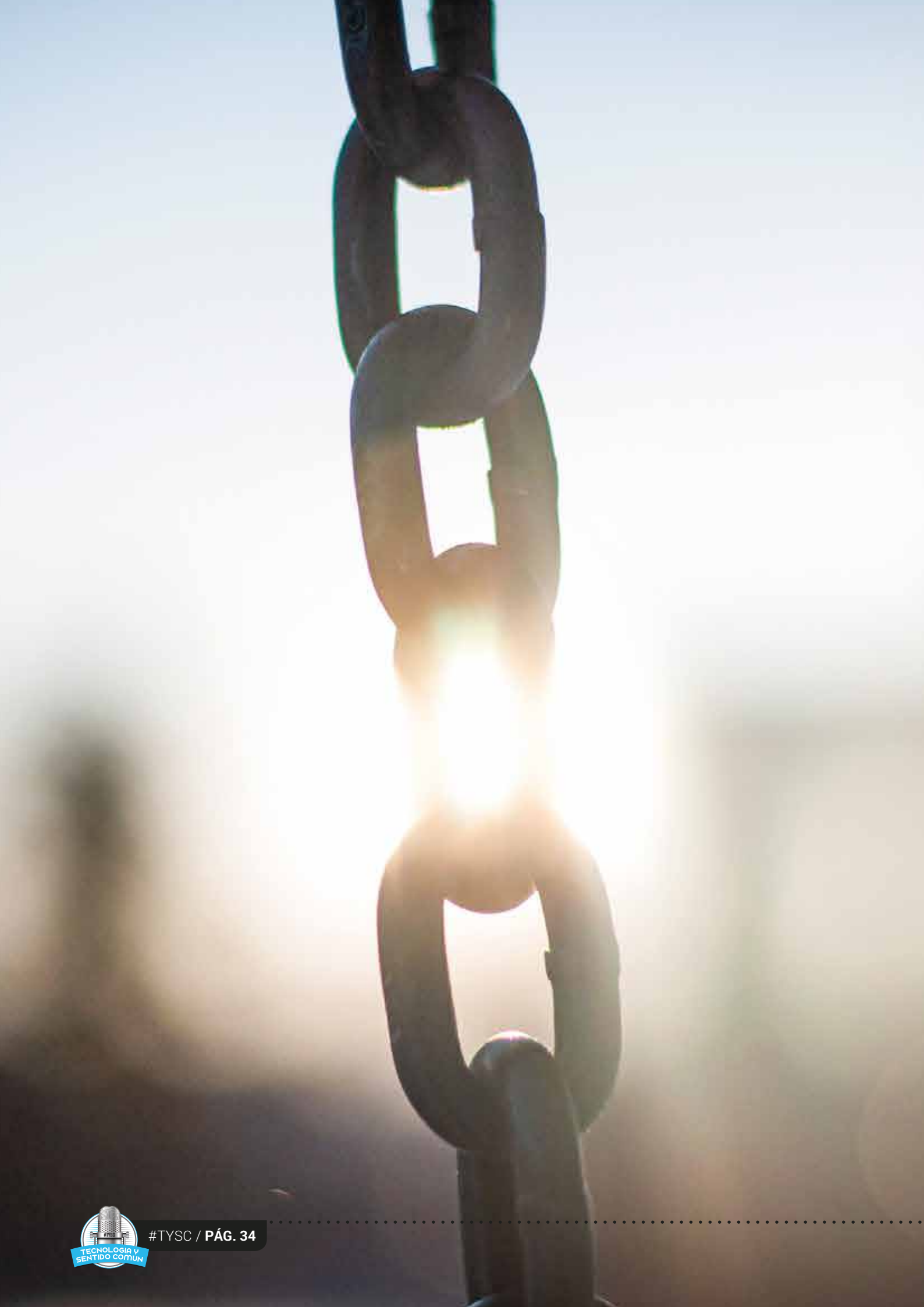
- Formación experiencial y participativa en remoto y en directo para una mayor comodidad del alumno.
- Cursos de cuatro sesiones en formato tardes de martes y jueves o formato viernes tardes y sábados mañanas.
- Máximo doce alumnos por convocatoria para una mayor interacción y compartición de experiencias 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



La criticidad de la cadena de suministro

En un entorno tecnológico cada vez más complejo, es evidente que existen múltiples relaciones entre organizaciones, que se prestan servicios o se suministran bienes entre ellas a cambio de determinadas contraprestaciones. En ese escenario, se pueden producir incidentes de ciberseguridad potencialmente desastrosos si alguno de los eslabones de esa cadena de suministros se ve comprometido. De ahí la importancia de la identificación y protección de todos los componentes de dicha cadena.

Hasta hace bien poco, los ejércitos movilizados se aprovisionaban mediante el pillaje en territorio enemigo, ya que no disponían de un mecanismo que suministrase víveres y demás pertrechos de forma continuada y '*just in time*'. Napoleón perdió su guerra en Rusia a principios del s. XIX (por el frío y) porque el ejercito imperial ruso no dejó ni una brizna de grano sin quemar en su retirada hacia Moscú, debilitando al ejército francés por inanición hasta que tuvo que retirarse con pérdidas enormes. De ésa y de otras campañas han aprendido los ejércitos modernos sobre la importancia de proteger sus vías de aprovisionamiento, y también a atacar o inutilizar las de sus enemigos, como una parte importante de sus estrategias de victoria.

En el entorno tecnológico y de ciberseguridad, cada vez son más las analogías que hacemos entre los enfrentamientos armados del Mundo Real™ y el ciberespacio. Usamos continuamente en el argot de la ciberseguridad palabras como 'amenaza', 'ataque', 'actor hostil', 'defensa', 'cortafuegos', etc. Y en esto del aprovisionamiento ha cobrado cierta importancia en los últimos tiempo la necesaria protección de la cadena de suministros tecnológicos. Ello es debido a que cualquier organización digitalizada hace uso de múltiples elementos que no ha construido ella misma, por razones obvia, por lo que ha recurrido a proveedores de bienes y servicios, tales como el acceso a Internet, sus proveedores de recursos en la nube, el fabricante de sus ordenadores, equipos de red o dispositivos móviles, etc.

Si son aún demasiado pocas las organizaciones que prestan una atención seria a la ciberseguridad, son aún menos las que prestan algo de atención precisamente a esa cadena de suministradores que permiten que su actividad se desarrolle con normalidad en el entorno digital[1]. Porque, ¿cuál sería el impacto de que un actor hostil incluyese algún tipo de malware o funcionalidad maliciosa en los equipos de red de una determinada organización? Las posibilidades que ofrecería ese escenario para dicho actor hostil son, a priori, muy atractivas. El equipamiento afectado podría funcionar aparentemente bien, pero estar capturando de forma transparente el tráfico de la red y enviándolo a un sistema externo. O simplemente, apagarse de forma destructiva ante una señal enviada por el actor malicioso, bloqueando las operaciones de la organización atacada.

CONTINÚA EN PRÓXIMA PÁGINA

O ¿qué pasa cuando nuestro proveedor cloud o de telecomunicaciones[2] es atacado y deja de prestar servicios con normalidad? De nuevo, la continuidad de nuestra organización se puede ver seriamente afectada. Sin embargo, es moneda corriente no considerar estos riesgos en las organizaciones, con el mantra de "es más fácil que me 'tumben' a mi el sistema que a *[proveedor- cloud-de-referencia]*". Mantra en el que hay un factor que se suele obviar: no hay ni el mismo interés ni el mismo número de agentes hostiles tratando de comprometer a los grandes proveedores de servicios que a una organización de tamaño pequeño o mediano, precisamente porque el impacto/beneficio obtenido en caso de un ataque exitoso es enorme. Además, esas empresas también tienen, a su vez, una extensa red de suministradores que deben mantener una elevada exigencia de ciberseguridad para que el gran proveedor cloud pueda ofrecer ese mismo nivel de seguridad a sus clientes. En este aspecto, se manifiesta una vez más aquello de que "una cadena es tan fuerte como su eslabón más débil".

De estas situaciones tenemos múltiples y recientes ejemplos, en las que no se ataca directamente a la organización objetivo, sino a uno de sus proveedores, 'envenenando' la cadena de suministros:

•Infectar con un ransomware a una miríada de empresas no tecnológicas a través de su proveedor de servicios TIC, que mantiene levantadas conexiones de VPN con ellas para prestarle sus servicios.

•Manipular maliciosamente un elemento software de uso corriente en otros productos software para disponer de un canal de acceso oculto a los sistemas de organizaciones que usen cualquiera de esos productos[3].

•Infectar los DNS de nuestro proveedor de acceso a Internet, redirigiendo todo el tráfico de sus clientes a través de sistemas donde dicho tráfico se analice para robar información bancaria, de contraseñas, o secretos industriales.

•Etc.

Por esa razón, es necesaria una adecuada protección de la cadena de suministro TIC de nuestras organizaciones. En las Administraciones Públicas españolas, el nuevo Esquema Nacional de Seguridad (aprobado en mayo de 2022) por fin cita la protección de la cadena de suministros explícitamente como una medida de protección. Dicha protección pasa por acometer acciones tendentes a reducir riesgos en dicha cadena, para lo cual se recomienda, al menos:

•Acortar y reducir la cadena de suministros, simplificando las relaciones externas de nuestra organización[4].

•Identificar/inventariar los elementos de nuestro entorno TIC y todos los componentes de los que depende o con los que está construido, de manera que sea más fácil identificar si una determinada vulnerabilidad nos afecta o no.

•Contratar con empresas que, a su vez, demuestren su compromiso con la protección de su cadena de suministro, y que apliquen políticas como las recomendadas.

•Mantener una adecuada vigilancia sobre todos nuestros activos, aunque hayamos delegado su gestión en un tercero, usando a otro tercero si es necesario.

•Integrar la cadena de suministro en nuestro Sistema de Gestión de la Seguridad de la Información corporativo.

Si pensamos, en la defensa de nuestros sistemas de información, como piensan los mandos de un ejército competente, analizaremos los riesgos, planificaremos las respuestas y nos aseguraremos que la cadena de suministro sea un riesgo controlado y asumible. No hay más.

REFERENCIAS

[1]https://www.zdnet.com/article/supply-chain-hacks-are-on-the-rise-but-most-companies-arent-prepared/
[2]https://www.antena3.com/noticias/tecnologia/ataque-informatico-proveedor-orange-deja-descubierto-datos-sensibles-clientes_2022110763693a75ac67a20001acab87.html
[3]https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
[4]https://www.itdigitalsecurity.es/endpoint/2022/09/las-extensas-cadenas-de-suministro-exponen-a-las-empresas-a-ataques-de-ransomware

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

La hemos liado parda. ¿y ahora qué?

En la revista de enero de 2023 de Tecnología y Sentido Común, Renato Aquilino planteaba, en su estupendo artículo mensual, los errores más comunes en lo que a continuidad de negocio se refiere. Esa continuidad de negocio suele enfocarse y planificarse frente a incidentes, pero puede provenir de otras fuentes menos 'canónicamente aceptadas' como tales: las fases de transición en la puesta en marcha de nuevos servicios o en cambios en esos servicios. Y recientes acontecimientos han puesto de relieve esa realidad. ¿Sirven los Planes de Continuidad de Negocio para atenuar los problemas en fase de transición? ¿Y qué hay de la comunicación a las partes interesadas?

La (a mi entender) 'redonda' versión de la librería de buenas prácticas ITIL v3 establecía una fase en el ciclo de vida del servicio denominada "Transición", en la que, "mediante la gestión y coordinación de recursos, procesos, sistemas y funciones requeridas, se evalúa, planifica, construye, prueba y despliega una versión de un servicio de tecnologías de la información (TI) en un entorno de producción". ¡Preciosa definición! Pero, ¿qué ocurre con la versión anterior, que se encuentra en fase de Operación en el momento en que el nuevo servicio está en fase de Transición? Ese servicio puede ser crítico para la organización, y muy probablemente, esté incluido en los planes de recuperación asociados al Plan de Continuidad de dicha organización, si lo tiene. Y llegará el momento en que se haya de detener el servicio versión X para poner en Operación el servicio en versión Y. Y ese momento, ¿estará en el Plan de Continuidad antes mencionado?

Nuestro compañero de revista, Renato Aquilino, describió en el número de enero de 2023 de Tecnología y Sentido Común [1], en un magnífico artículo, los errores más comunes en lo que caen las organizaciones en lo que a continuidad de negocio se refiere. Y seguro que estará de acuerdo conmigo en que si mezclamos en una coctelera la continuidad de negocio, la transición hacia nuevas versiones de servicios, la gestión del cambio y la necesidad de que las partes interesadas conozcan aquellos aspectos de estas cuestiones que les afecten directamente, nos encontraremos ante una situación especial, sobre todo, cuando las cosas no van según lo planificado.

Tras el paso de la versión X a la versión Y de un servicio, ¿se habrá actualizado el Plan de Continuidad y los documentos de detalle que lo conforman, para ajustarlo a la nueva situación? En caso de que la transición de la versión X a la versión Y del servicio sea fallida o se salga de la ventana de actualización establecida, ¿tendrá claro el personal técnico qué plan de recuperación han de ejecutar, o cuál debe ser la estrategia de comunicación?

CONTINÚA EN PRÓXIMA PÁGINA

En enero de 2023, hemos sido testigos de situaciones en las que se ha puesto de relieve esta relación entre la fase de transición, la gestión del cambio y la continuidad de negocio. Una compañía aérea española [2], y nada más y nada menos que Microsoft [3], han sufrido casos de indisponibilidad de sus servicios y operaciones debidos a caídas de sus sistemas de información. Asimismo, una entidad financiera española [4] planificó una determinada intervención de mantenimiento y actualización de sus sistemas. Al parecer, la actividad no fue según lo planeado, y el resultado fue una indisponibilidad de sus sistemas de varios días, algo que, ***per se,*** es bastante grave en una entidad de ese tipo. Quede claro en este punto que no soy cliente ni accionista de dicha entidad ni de ninguna de la competencia, y que por ello me permito hacer el análisis que sigue. Me consta el estupendo trabajo y dedicación que el equipo de TI de la entidad realizó en ese periodo de corazones acelerados por la incertidumbre, en una situación organizativa compleja, y acompañados de sus proveedores de servicios, para dar la mejor y más rápida solución a la cuestión.

Sin embargo, desde el punto de vista de sus clientes (una de sus partes interesadas), se produjo un fallo de comunicación en el caso de la entidad financiera, que no se dio en los otros dos casos citados, ya que las quejas mayoritarias en redes sociales durante esos días fueron, precisamente, porque la entidad no fue transparente con sus clientes, explicando con cierto detalle cuál era el problema. Ello llevó, y más en estos tiempos de bulos y desinformación, a la propagación de todo tipo de rumores, sobre todo, en relación a un posible incidente de ciberseguridad grave en la entidad. Los desmentidos tardíos, a juicio de lo que se pudo leer en esas fechas en las redes sociales, no tranquilizaron a sus clientes, precisamente en un negocio que se basa en la confianza del cliente, que deposita en la entidad bancaria su dinero o el de su empresa, y que utiliza los servicios de banca electrónica de manera permanente.

A buen seguro que el Plan de Continuidad de esa entidad estará perfectamente redactado y las responsabilidades del mismo perfectamente definidas. Los planes de recuperación de cada sistema estarán documentados al detalle, y se habrán realizado simulacros, pruebas y briefings de lecciones aprendidas para mejorarlos en tiempo y forma. Pero en los entornos tecnológicos, y sobre todo si nuestra organización debe dar la cara ante el público en general, en ocasiones no somos conscientes, centrados en nuestra tarea tecnológica, de la importancia de comunicar lo que ocurre y lo que se está haciendo para resolverlo, porque ese es un rasgo que genera confianza en el cliente, reduce la posibilidad de que se cree desinformación alrededor del incidente, y reduce el impacto reputacional negativo que sufriremos.

Y es que en estos tiempos nos hemos acostumbrado a la mentira, la sospecha y la conspiranoia, y de cualquier cosa se hace un mundo, gracias a la amplificación de las redes sociales y de ciertos 'medios de comunicación' (sic) que alimentan todo tipo de bulos. Frente a ello, una comunicación controlada, pero sincera y transparente con las partes interesadas, es la mejor herramienta. En el caso que nos ocupa, quizá haber avisado antes de las tareas a los clientes les hubiera permitido prever la realización de ciertas operaciones antes de la intervención. También hubiera estado bien informarles de cuáles eran los tiempos previstos de resolución del incidente cuando éste ya estaba de manifiesto públicamente.

Por tanto, me permito el lujo, con el permiso de mi compañero de revista Renato Aquilino, en añadir un error más a los que él detallaba en el artículo al que me he referido antes:

[ERROR 5] La hemos liado parda. ¿Ahora qué?

Los Planes de Continuidad han de tener en cuenta no sólo incidencias fortuitas o de actores externos, sino que han de tener en cuenta también las tareas de transición para la puesta en marcha de nuevos servicios o actualización de servicios o sistemas. Además, en los Planes de Continuidad se ha de prestar atención especial a la estrategia de comunicación, para tratar de minimizar el impacto reputacional que el incidente que da lugar a la aplicación del Plan de Continuidad pueda tener en la organización. Y esa estrategia de comunicación debe ajustarse a cada una de las partes interesadas, ya que no es igual ni el tipo, ni la cantidad de la información remitida, ni la periodicidad de su envío, si el receptor es el CEO de la entidad o uno de sus clientes.

En conclusión, planifiquemos, ejecutemos y no olvidemos comunicar eficientemente.

Referencias

[1]https://tecnologiaysentidocomun.com/ipages/flipbook/revista-tysc26-enero-2023 págs. 68-70.
[2]https://www.xataka.com/otros/iberia-sufre-caida-sus-sistemas-que-ha-provocado-cancelaciones-vuelos-retrasos
[3]https://www.elcorreo.com/tecnologia/caida-mundial-microsoft-servidor-afecta-millones-usuarios-20230125100122-nt.html
[4]https://cincodias.elpais.com/cincodias/2023/01/20/companias/1674229689_795812.html

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

¿Es un bulo? ¿Es un Deep Fake? Sí, Es Malinfo

Recientemente llegó a mis oídos el término MALINFO, para referirse a todo tipo de información no ajustada a la verdad. Es este término se agrupan multitud de manifestaciones que tratan de confundir, engañar o manipular a quien las lee, las ve, o las escucha, a través de varios medios. Pero, aparte de las típicas estafas, las iniciativas de MALINFO ¿qué buscan? Este mes lo analizaremos en este artículo.

Hace un tiempo tuve la oportunidad de publicar, en otro medio, un artículo acerca del fenómeno de las *fake news*[1] . Ya en ese artículo de hace casi tres años me posicionaba al identificar a los bulos (o fake news) de cualquier tipo como una amenaza a la convivencia y la democracia, y explicaba algunos de los mecanismos que favorecen la diseminación de este tipo de informaciones falsas. Incluso daba mi opinión sobre la posibilidad de que ese tipo de actividades tuvieran una sanción desde el punto de vista penal, dada su peligrosidad.

Con motivo de un curso al que asistí recientemente, uno de los formadores utilizó el término MALINFO, y la verdad es que es una expresión que resume perfectamente el tipo de fenómeno al que se enfrentan las sociedades democráticas, y que aúna además connotaciones que recuerdan al concepto de malware. En ese término MALINFO podemos agrupar a los bulos, o las fake news, que proliferan en los diferentes servicios de Internet, e incluso, las mentiras interesadas o medias verdades que nos estamos acostumbrando a ver en los medios de comunicación tradicionales. Medios que, en muchos casos, han dejado de ser de comunicación para transformarse en medios de manipulación de masas.

Conscientes de ello, los gobiernos de los diferentes países se afanan en protegerse de este fenómeno, ya que resulta obvio que puede ser aprovechado por intereses extranjeros para debilitar sus democracias o crear estados de opinión favorables a sus intereses. Porque la manipulación de la opinión pública es una "ciencia" (sic) que viene de antiguo, y en la que el régimen de la Alemania nazi elevó a la "excelencia", de la mano de Joseph Goebbels. Pero ¿qué pueden hacer los estados liberales frente a esta marea de informaciones falsas que tratan de dañarles?

Por lógica, lo primero que hay que hacer es identificar las diferentes modalidades de la amenaza. Estaremos todos de acuerdo en que no es lo mismo un bulo del tipo "va a subir el producto X", por más que los ejércitos de bots en redes sociales lo repitan, que un deep fake de la presidenta de un país en el que anuncie la declaración de una guerra contra el país vecino. Y lamentablemente, cada vez más vemos que los avances en inteligencia artificial facilitan enormemente este tipo de amenazas. Hay ya productos de inteligencia artificial

CONTINÚA EN PRÓXIMA PÁGINA

que pueden replicar la voz y las emociones de cualquier persona simplemente escuchandola hablar tres segundos[2], por lo que algunas de las escenas de la saga cinematográfica Terminator ya serían posibles en la actualidad (las menos violentas, al menos). Urge, por tanto, una regulación de los usos éticos de la Inteligencia Artificial lo más universal posible, al igual que ocurre con ciertas parcelas de la investigación biomédica. Por más que una regulación ética no hubiera impedido el éxito de empresas cuya actividad saltó a la luz pública en febrero de 2023[3], que se vanaglorian de utilizar todo tipo de medios para manipular elecciones en una multitud de países.

Identificadas las posibles formas de la amenaza, lo siguiente debería ser intentar identificar los destinatarios de la misma, es decir, aquellos colectivos que pueden verse influenciados por la información falsa publicada. Un gobierno dispone de medios para hacer llegar la información verídica a los afectados, aunque también es cierto que uno de los primeros objetivos de cualquiera de estas campañas es siempre minar la confianza y la legitimidad de dicho gobierno, como vacuna contra la información real. De ahí que sea muy importante identificar estas campañas en sus inicios y cortarlas de raíz. Y en esa actividad es crítico la utilización de técnicas de inteligencia de medios sociales (o SOCMINT), que deberían, además, identificar el origen de esos bulos más pronto que tarde.

Por supuesto, es necesaria una decidida acción en los medios de comunicación tradicionales que, voluntaria o involuntariamente, dan pábulo a esas campañas de MALINFO, con la excusa de la libertad de prensa, contraponiendo datos con el relato falso. Ello, claro está, en el supuesto de que la información que pretende dar ese gobierno sera veraz y sincera, por que lo contrario generaría un efecto rebote que daría más credibilidad a las *fake news*.

Los ciudadanos, en general, tampoco debemos 'escurrir el bulto' ante este problema, y de la misma manera que se toman precauciones para no facilitar la expansión de virus (biológicos o informáticos), debemos tener precaución con la información que compartimos. Por más que una información refuerce nuestro sesgo ideológico/religioso/económico, comprobarla antes de darle publicidad irá en beneficio de todos. El sentido crítico ante ciertas noticias, videos, o audios, protegerá nuestras democracias liberales de los intentos de desactivarlas, como se ha visto en los últimos tiempos con las campañas de desinformación relacionadas con la invasión rusa de Ucrania[4]. En ese aspecto, la Unión Europea tomó valientes decisiones, prohibiendo la difusión de los medios de (des)información rusos, que pretendían manipular a la opinión pública europea a su favor, para evitar el apoyo occidental al país invadido.

Y la tecnología también puede hacer su parte, ya que del tratamiento lo más automatizado posible de la información recopilada sobre determinadas campañas, de su depuración y de su destilación, se debería obtener un conocimiento del quién, el porqué, el cómo y el cuándo que permitiera una acción policial o judicial que detenga la campaña o prevenga que se desarrollen nuevas campañas de MALINFO. Por ello es esencial que los países dispongan de buenos analistas de OSINT (Open Source Intelligence)[5] y SOCMINT enfocados en diferentes niveles de la administración. Porque no nos engañemos: las campañas de desinformación se pueden gestar a todos los niveles, desde el más pequeño ayuntamiento hasta a nivel global.

El 7 de febrero se celebró el Día de la Internet Segura, y una de las necesidades a cubrir para que eso sea así es acabar con la MALINFO. Todos podemos ser parte del problema, o mejor, ser parte de la solución. Sólo nos hace falta la actitud correcta y pensar en el bien superior a proteger.

Referencias

[1]https://www.computerworlduniversity.es/ciberseguridad/mentiras-bulos-y-fal
ews-en-un-mundo-digital
[2]https://www.genbeta.com/herramientas/esta-ia-microsoft-puede-imitar-voz-e
ciones-persona-a-partir-audio-tres-segundos-asi-funciona-vall-e
[3]https://www.businessinsider.es/team-jorge-grupo-hackers-ha-manipulado-30
cciones-1200784
[4] https://www.newtral.es/desinformacion-rusa-ucrania-seis-meses/20220824/
[5]https://tecnologiaysentidocomun.com/ipages/flipbook/revista-tysc18-abril-2
págs. 12-14

Stakeholders.news

Cada tercer domingo de mes disfruta de la Revista Stakeholders.news
Revista Mensual de los Profesionales en Dirección y Gestión de Porfolios, Programas y Proyectos, Cambio Organizacional y Transformación Digital.

La (Ciber)seguridad de los vehículos conectados

Los automóviles llevan ya bastantes años cumpliendo con unos exigentes estándares de seguridad activa y pasiva, casi obsesionados en proteger a sus ocupantes en caso de colisión. Pero también, de un tiempo a esta parte, los vehículos han comenzado a llevar una multiplicidad de equipos electrónicos embarcados, conectados entre sí mediante redes de tipo industrial, para, finalmente, conectar el vehículo a Internet para la obtención de determinados servicios de la Red. Analicemos los problemas que esto acarrea para la seguridad de los ocupantes del vehículo.

Lejos están los tiempos en que los vehículos funcionaban únicamente con elementos mecánicos, ya que comenzaron a incorporar componentes electrónicos en diferentes subsistemas. Con la popularización de la electrónica digital de consumo, los vehículos comenzaron a integrar Unidades Centrales Electrónicas (o ECUs, por sus siglas en inglés), interconectadas a través de redes industriales, como CAN o ModBus. Además de controlar diferentes

aspectos de la mecánica y la conducción del vehículo, las ECU extendieron su uso a lo que se conoce como 'infotainment', o equipamiento de información y entretenimiento, que finalmente ha conectado a Internet estos vehículos. Y a esta alturas ya todos deberíamos saber que algo conectado a Internet se convierte en algo amenazado y candidato a ser atacado por diversas motivaciones. Lo grave, en este caso, es que eso podría afectar a la vida de los ocupantes del vehículo.

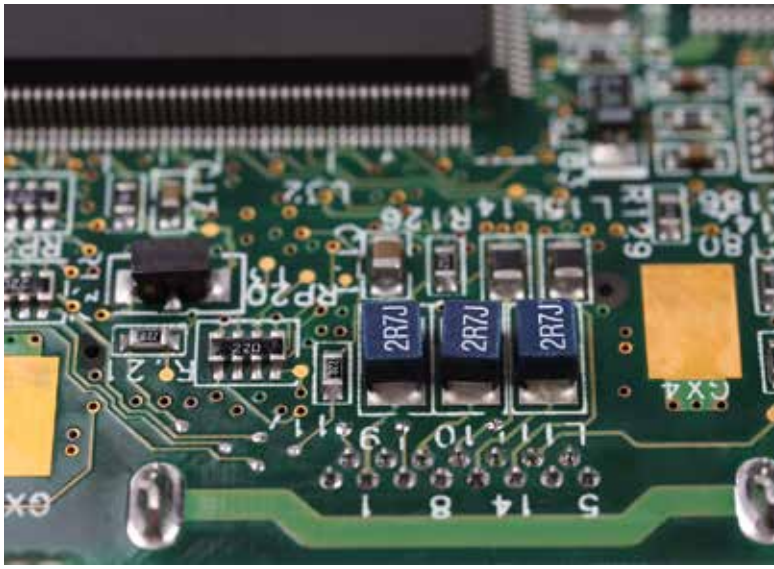
La primera fuente de vulnerabilidad de los vehículos electrónicos, estén o no conectados a Internet, es el software que se encuentra integrado en cada una de las ECU. Datos de 2014[1] reflejaban el hecho de que un vehículo de la época ya integraba 100 millones de líneas de código entre sus diferentes ECUs, lo cual, comparándolo con los 2 millones de líneas de código del caza F-22, los 50 millones del LHC del CERN, o los 61 millones de Facebook, dan una idea de la complejidad del software con el que funcionan los coches modernos. Cualquier software es candidato a contener errores o vulnerabilidades, ya que es matemáticamente imposible demostrar que un software esté libre de errores. Por tanto, un software de 100 millones de líneas puede tener un elevado número de errores, aunque los estándares de calidad de la industria automotriz los puedan reducir muchísimo en las fases de prueba previas a la liberación de ese software en una ECU de mercado. ¿Qué podría ocurrir si, en plena marcha a 120 km/h, un error indetectado del software de a bordo provocara un comportamiento errático

CONTINÚA EN PRÓXIMA PÁGINA

del vehículo, o que se reiniciara una o varias ECUs? ¿Quién sería responsable del accidente? ¿El conductor? ¿El fabricante del vehículo? ¿El fabricante del software de la ECU? ¿De cual de ellas?

La segunda fuente de vulnerabilidad de los vehículos modernos son sus puertos físicos de comunicaciones, como el OBD2[2]. A través de este puerto, pensado como puerto de diagnóstico para las ECUs del vehículo, se puede obtener información de las diferentes redes del vehículo. Y quien dice obtener, dice inyectar o modificar. Imaginemos que un agente malicioso accede al vehículo y coloca en el interfaz OBD2 un elemento que, de forma remota, permita a dicho agente manipular la información que las diferentes ECUs intercambian. Podría hacer que el vehículo acelerara en lugar de frenar, o el volante girara a la derecha en lugar de a la izquierda. En resumen, dispondría de control casi total sobre el vehículo y, por tanto, sobre sus ocupantes. ¿Recuerda el lector aquello de "Que parezca un accidente"? Puede ser el sueño húmedo de cualquier asesino a sueldo del crimen organizado. Y no crea el lector que esto es ciencia ficción. Quien les escribe ha podido acceder a videos en los que un grupo de investigadores en ciberseguridad manejaban en remoto un vehículo de serie, conduciéndolo, desbloqueando funcionalidades de motorización que están en el vehículo pero que el fabricante sólo desbloquea mediante el correspondiente pago, etc.

La tercera fuente de vulnerabilidad de los vehículos electrónicos seguro que el lector ya se la imagina: su conexión a Internet. Conexión a través de la cual, obviamente, se podría acceder al vehículo remotamente, sin las adecuadas medidas de seguridad. A partir del momento en que un vehículo se conecta a Internet, está expuesto al mismo tipo de riesgos que cualquier otro dispositivo. Un agente malicioso podría modificar la información del GPS de determinados modelos de vehículos de alta gama para redirigir sus rutas hacia lugares en los que poder interceptar esos vehículos y robarlos, atracar a sus ocupantes o incluso secuestrarles. Un atacante remoto podría monitorizar a diferentes vehículos como mecanismo de vigilancia hacia sus ocupantes, y vender esa información a grupos rivales o empresas competidoras. Y por supuesto, sin las medidas de seguridad oportunas, podría acceder a las redes industriales del vehículo y controlarlo, al estilo de lo indicado anteriormente para el puerto OBD2.



Visto lo visto, ¿qué podría ocurrir en el siguiente paso de la evolución de los vehículos conectados, cuando se popularice la conducción autónoma? Subirse a uno de esos vehículos que haya sido vulnerado podría ser una sentencia para los ocupantes, ignorantes de los riesgos a los que se enfrentarían. En estos vehículos, además de todo lo contado para el vehículo conectado, nos encontramos con que se trata de verdaderos robots con ruedas, equipados con sistemas de inteligencia artificial, entrenados vaya usted a saber con qué sesgos en su algoritmo, y cuya percepción y toma de decisiones puede ofuscarse también por la acción de un actor malicioso.

Dicho todo esto, hay que recalcar que la industria automovilística no es desconocedora de la problemática, y que desde hace unos pocos años está poniéndose manos a la obra para proteger a sus clientes, por lo que volveremos a ver un episodio más de la competición entre los expertos en ciberseguridad y los ciberdelincuentes, esta vez en el campo de batalla de los vehículos inteligentes. Pero como en otros ámbitos, como la industria 4.0 o el IoT, en esta pelea hay vidas en juego, por lo que la rigurosidad de las medidas y la calidad del software a implementar han de ser máximas.

Eso es lo que todos esperamos.

Referencias

[1] https://www.linkedin.com/pulse/20140626152045-3625632-car-software-100m-lines-of-code-and-counting
[2] https://www.diariomotor.com/que-es/obd2/

12 MESES GRATIS

NUEVO PROGRAMA DE DIGITALIZACIÓN DISPONIBLE

Programa ITSM

Implementa uno de los ITSM más completos de todo el mercado europeo a un coste 0€ (paquete básico)

¿Por qué elegir ITSM de Efecte?

1. Contamos con más de 20 años de experiencia.
2. Plataforma low-code, fácil de usar y muy gráfica.
3. Efecte es el único proveedor que ofrece 12 meses de uso GRATIS.
4. Ofrecemos ayuda experta gratuita y a medida, antes, durante y después de la implementación.

El proceso de selección de empresas ya está abierto y las plazas son limitadas. ¡DATE PRISA!

MÁS INFORMACIÓN

efecte

www.efecte.es

Cibercrimen, a la orden del día

Ya en el primer número de Tecnología y Sentido Común abordamos el tema del cibercrimen. Dos años y medio después, la situación, lejos de mejorar, parece que empeora en ese ámbito, ya que cada vez son más los delitos que tienen lugar en el mundo digital, o que se aprovechan de él para facilitar su comisión o dificultar su represión. Merecía, la pena, por tanto, revisitar este tema a la luz de estas cuestiones.

El cibercrimen ya no es lo que era. Ya no son chalados queriendo cambiar sus notas de clase o jugar gratis a videojuegos, como en la película clásica Juegos de Guerra (1983), ni tampoco son gente solitaria y encapuchada, como el personaje de Neo en Matrix (1999). Las cosas han cambiado mucho, y esos cambios se han acelerado en los últimos años.

Ya hemos escrito en esta sección acerca del cibercrimen, por ejemplo, en el n.º 1 de esta revista, allá por octubre de 2020. Hemos escrito también acerca del Ransomware-as-a-Service, en el n.º de octubre de 2021, todo un ecosistema empresarial ilegal alrededor de la actividad de cifrar, y últimamente exfiltrar, los datos de las organizaciones atacadas, pidiendo un rescate a cambio de la clave de descifrado y de no revelar los datos robados. También hemos mencionado los problemas que para la ciberseguridad suponen los grupos de ciberdelincuentes patrocinados (presuntamente) por estados como Rusia, China,

Corea del Norte o Irán, más si cabe conforme las capacidades aumentan y se permiten atacar infraestructuras como plantas potabilizadoras de agua, sistemas de generación eléctrica o entornos domóticos de edificios. Y en estos años se ha pasado del cibercrimen a la ciberguerra, algo que se ha manifestado en toda su crudeza con la invasión rusa de Ucrania.

En paralelo al crecimiento del cibercrimen (y de las acciones de ciberguerra) han crecido las capacidades de los estados desarrollados para su ciberdefensa, al igual que la colaboración entre países en este ámbito. Por ejemplo, en España disponemos de un Plan Nacional de Ciberseguridad, de unidades policiales especializadas, tanto en la Policía Nacional como en la Guardia Civil, un Mando Conjunto del Ciberespacio y un excelente nivel de colaboración con el sector privado. Pero pese a todo, en estos años hemos vivido episodios de cibercrimen que nos han hecho sonrojar como país. Y no por falta de esfuerzo ni de dedicación de los responsables de la ciberseguridad, sino porque quienes están enfrente disponen de muchos recursos, tienen claro su objetivo y sólo han de encontrar un resquicio para que todo salte por los aires.

Hoy en día el cibercrimen que sale en las noticias lo perpetran, en su mayoría, grupos organizados, igual que ocurre con el tráfico de drogas, de armas o de personas. Son grupos que cuentan con verdaderos departamentos de investigación y desarrollo, departamentos de 'atención al cliente', etc. Son una estructura empresarial fuera de la ley, que opera internacionalmente y se aprovecha de las criptomonedas y las fronteras para hacer florecer su negocio.

Sin embargo hay un cibercrimen 'de baja intensidad', el que realizan los estafadores de poca monta, que han adaptado su modus operandi a las nuevas plataformas de venta on line entre particulares, sin ir más lejos, y que ha crecido como la espuma en los últimos años. Productos que se pagan y no llegan, identificaciones falsas para generar una sensación de falsa confianza, servicios que se cobran y no se prestan nunca, etc. En todos estos casos, el delincuente trata de que la víctima realice el pago fuera de los canales oficiales de la plataforma a través de la que han contactado, para evitar así los controles que estas plataformas plantean, conocedoras del riesgo reputacional que pueden afrontar en estos casos.

CONTINÚA EN PRÓXIMA PÁGINA

También hay otras variantes de cibercrimen que son menos percibidas como tal. Por ejemplo, las personas que intentan irse sin pagar de un restaurante amenazando con ponerles malas críticas que van a leer sus seguidores en diferentes servicios on line y redes sociales. Es un caso de extorsión o chantaje, pero raramente se enfoca de esa manera, al ser la cantidad que se exige en especie y no demasiado alta.

Entidades como la Oficina de Seguridad del Internauta de INCIBE, o los cuerpos policiales, regularmente hacen campañas de concienciación para los ciudadanos, pero parece que su éxito no es el esperado, por lo que se han de redoblar los esfuerzos en ese ámbito. Sin embargo, y como la naturaleza humana es así, somos blanco fácil para los ataques de ingeniería social, y lamentablemente este tipo de cibercrimen de baja intensidad está lejos de erradicarse. Como dicen en ciertos ambientes investigadores, hay que 'seguir el dinero' (*follow the money*) para llegar a atrapar al delincuente, pero la propia tecnología hace que a veces esto sea muy difícil de lograr.

Porque hay otro fenómeno a citar: el del número de ciberdelitos que no se llegan a denunciar precisamente porque se piensa que no se va a poder hacer nada al respecto, o por la sensación de vergüenza que la víctima tiene por haberse dejado engañar. Y éste es otro ámbito en el que debemos concienciar a los ciudadanos: denuncien. Quizá su denuncia no llegue a ningún lado, o quizá sí, y se eviten futuros delitos.

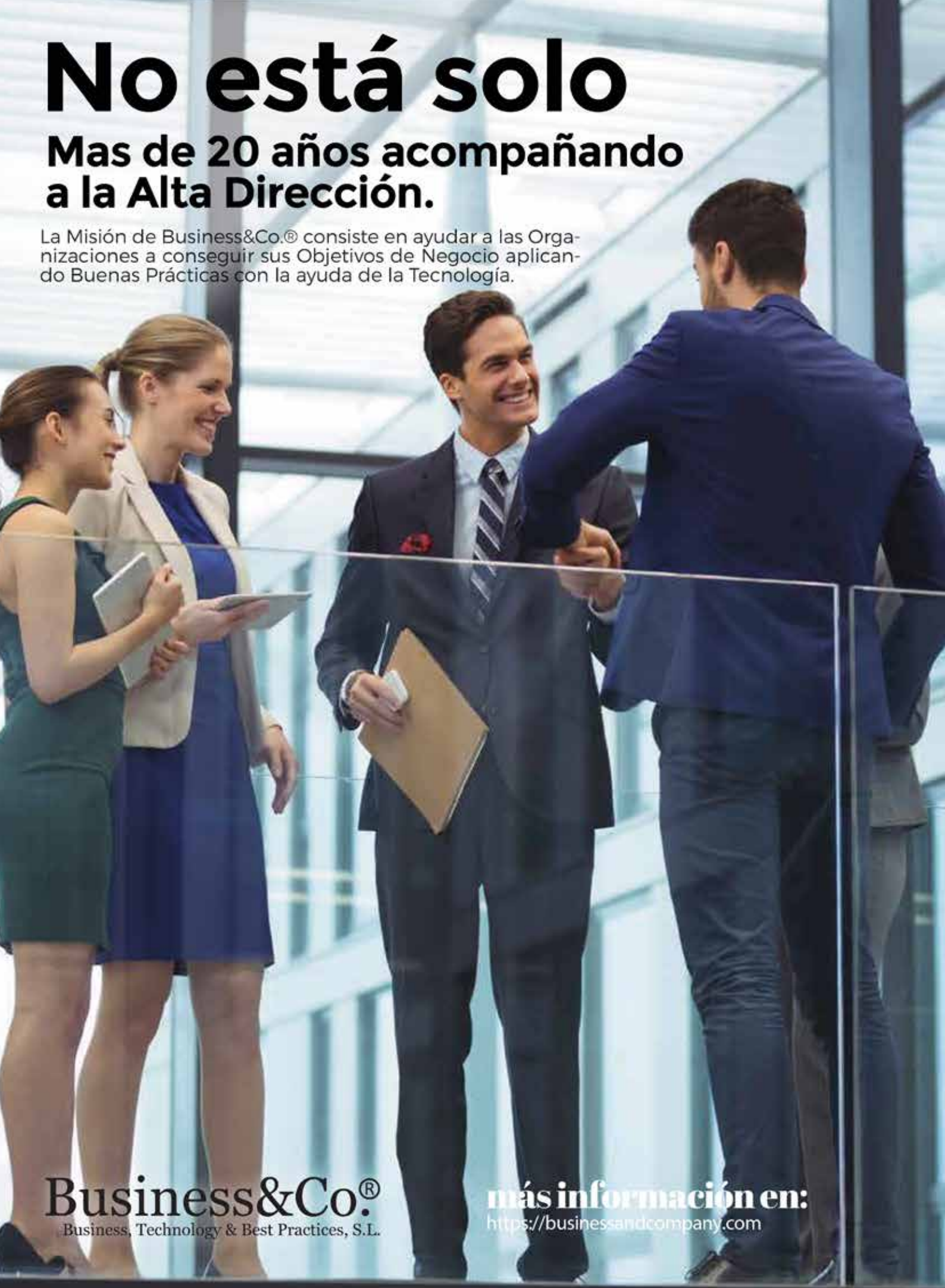
Como ya escribí en su día, luchar contra el cibercrimen es tarea de todos, y más cuánto más se digitaliza nuestra sociedad. No perdamos la oportunidad de advertir a nuestras amistades, conocidos o seguidores en redes sociales sobre estafas, timos, bulos, campañas de malware en curso, etc. Tal vez nos tilden de pesados, pero si podemos evitar que algunos ciudadanos no sean víctimas de un ciberdelito, bienvenido sea el epíteto.

No todos los héroes llevan capa. No lo olviden.

No está solo

Mas de 20 años acompañando a la Alta Dirección.

La Misión de Business&Co.® consiste en ayudar a las Organizaciones a conseguir sus Objetivos de Negocio aplicando Buenas Prácticas con la ayuda de la Tecnología.



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

más información en:
https://businessandcompany.com

Business&Co.®, Escuela de Gobierno eGob®, Master en Gobierno de Tecnologias de la Información MGEIT®, Caviar®, Telecoms®, Respalda® y AulaDatos® son Marcas y Nombres Comerciales Registrados de Business, Technology & Best Practices, S.L.

Ciberseguridad nacional: todos a una

En este último artículo de la octava temporada de Tecnología y Sentido Común, antes del paréntesis vacacional, trataremos de dar a conocer a nuestros lectores cómo se estructuran los diferentes aspectos de la seguridad nacional española, en el ámbito de la seguridad de los sistemas de información y las infraestructuras críticas. Un entorno en el que operan diversos organismos para tratar de proteger a nuestro país y a sus habitantes de las amenazas de origen tecnológico.

A estas alturas, el lector de nuestra revista ya sabe perfectamente lo complejo que resulta el mundo de la ciberseguridad, y los diferentes tipos de actores y amenazas presentes en el mismo. No en vano son muchos los artículos que hemos publicado relacionadas con la temática indicada. Sin embargo, no son pocas las personas, e incluso algunos profesionales del sector, que tienen la sensación de que están solas ante el peligro.

En España, y como ya informamos en nuestro artículo de mayo de 2022, disponemos de un Plan Nacional de Ciberseguridad aprobado por el Gobierno, en el que se detallan las acciones a llevar a cabo para tratar de proteger a nuestro país de las amenazas del ciberespacio. La ejecución de ese plan corre a cargo de diferentes estamentos, con la colaboración del sector privado, y es interesante conocer los ámbitos de actuación de cada uno de ellos y las competencias que tienen, porque ello redundará en una mayor confianza del ciudadano.

Dado que muchos delitos se están cometiendo utilizando las tecnologías de la información y las comunicaciones, desde hace ya bastantes años tanto la Policía Nacional como la Guardia Civil disponen de unidades específicas para perseguir y combatir los ciberdelitos. Según su web, "*La **Brigada Central de Investigación Tecnológica** está encuadrada en la Unidad de Investigación Tecnológica (...) que es el órgano de la Dirección General de la Policía encargado de la investigación y persecución del ciberdelito de ámbito nacional y transnacional. Actuará como Centro de Prevención y Respuesta E- Crime de la Policía Nacional". Asi mismo, "el **Grupo de Delitos Telemáticos** fue creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos delitos que se cometían a través de Internet, y su origen se remonta al año 1.996*". Por tanto, si somos víctimas de un delito que involucre las TIC como forma de comisión, podemos plantear denuncia ante cualquiera de los dos cuerpos policiales, y serán sus respectivas unidades especializadas quienes lo investigarán.

En el ámbito militar, el ciberespacio se ha convertido en un nuevo teatro de operaciones, donde es complejo diferenciar entre el "simple delito" y las operaciones encubiertas de ciertos países hostiles. Por ello, en España "*el **Mando Conjunto del Ciberespacio** es el órgano responsable del planeamiento, dirección, coordinación, control y ejecución de las acciones conducentes a asegurar la libertad de acción de las Fuerzas Armadas en el ámbito ciberespacial. Para cumplir su misión, planeará, dirigirá, coordinará, controlará y ejecutará las operaciones militares en el ciberespacio, de acuerdo con los planes operativos en vigor. En el ámbito de estas operaciones, realizará las acciones necesarias para garantizar la supervivencia de los elementos físicos, lógicos y virtuales críticos para la Defensa y las Fuerzas Armadas*". Una estupenda definición en la que se deja clara la importancia que tiene para la defensa nacional que los cuerpos militares dispongan de una adecuada organización para la Ciberdefensa y la Ciberguerra.

La información es poder, y la ciberinteligencia es uno de los ámbitos en los que actúa el **Centro Criptológico Nacional (CCN)**, encuadrado en el Centro Nacional de Inteligencia (CNI), dependiente de la Presidencia del Gobierno de España. Este organismo es una de las piezas fundamentales de la ciberseguridad del sector público nacional, ya que es el encargado de facilitar la aplicación del Esquema Nacional de Seguridad, para lo cual ofrece una panoplia de servicios, en colaboración con el sector privado, tales como (según su web):

•"(…) Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas TIC (Guías CCN-STIC).
•(…) Formar al personal del Sector Público especialista en el campo de la seguridad.
•(…) Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia.
•(…) Coordinar la promoción, desarrollo, obtención, adquisición y puesta en explotación y uso de tecnologías de seguridad.
•(…) Valorar y acreditar la capacidad de los productos de cifra y de los sistemas para manejar información de forma segura.
•(…) Contribuir a la mejora de la ciberseguridad española, a través del CCN-CERT, afrontando de forma activa las amenazas que afecten a sistemas del Sector Público, a empresas y organizaciones de interés estratégico para el país,(…) y a cualquier sistema TIC que procese información clasificada."

CONTINÚA EN PRÓXIMA PÁGINA

Para el sector privado, en España disfrutamos de los servicios del Instituto Nacional de Ciberseguridad (INCIBE), una sociedad estatal cuya misión es "*mejorar la ciberseguridad y la confianza digital de ciudadanos, menores y empresas privadas de España; proteger y defender a los ciudadanos, menores y empresas privadas; potenciar la industria española de la ciberseguridad, impulsando la I+D+i española en ese campo, e identificar, generar, atraer y desarrollar profesionales del sector de ciberseguridad*."

Finalmente, hay otro organismo con funciones relacionadas con la ciberseguridad, y es el Consejo Nacional de Protección de Infraestructuras Críticas (CNPIC). La Directiva europea 2008/114/CE del 8 de diciembre de 2008 establece por infraestructura crítica "*el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población, cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones*". Resulta obvio que no podemos hacer uso del ciberespacio si no disponemos de redes de comunicaciones funcionales, o si no disponemos de fluido eléctrico, y para su protección, entre otras, se creó el CNPIC y la normativa oportuna. El CNPIC "*es el órgano responsable de la dirección, coordinación y supervisión de la protección de infraestructuras críticas nacionales. Por ello, es el encargado de dirigir la aplicación del Plan Nacional de Protección de Infraestructuras Críticas y se convierte en el punto nacional de contacto con la Comisión Europea y con otros Estados propietarios o gestores de infraestructuras críticas*".

Finalmente, hablemos de la coordinación de todos estos organismos que hemos citado en el artículo, ya que sin ella los esfuerzos podrían duplicarse o no llegar a cubrir a todos los implicados. **El Consejo Nacional de Ciberseguridad** es el órgano colegiado de apoyo al Consejo de Seguridad Nacional (...), y está presidido por el secretario de Estado director del CNI. (...) es el encargado de reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privados, y facilita la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional".

Todos somos parte en esta cuestión de la ciberseguridad, como hemos mencionada ya en varias ocasiones. En resumen, **sólo no puedo, pero con amigos, sí**.

Tecnología y Sentido Común volverá, como es habitual, el primer fin de semana de septiembre. Hasta entonces, les deseo que descansen, que se relajen, y que disfruten de sus merecidas vacaciones, pero no dejen de permanecer en alerta. Los malos no descansan.

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

Lanzamiento del Service Management Institute SMI®

El miércoles 26 de abril tuvo lugar el lanzamiento del Service Management Institute SMI®, la comunidad global de profesionales en la Dirección y Gestión de Servicios, Comprometidos con la Innovación, las Buenas Prácticas y la Mejora Continua.

Este acto fue la escenificación de la transformación de la Asociación sin Ánimo de Lucro itSMF España, asociación profesional que desde el año 2004 ha atendido las necesidades de la Gestión de Servicios de Tecnología (ITSM), y que a partir de 2023 se renueva para atender los servicios de una forma global en todas las áreas de la empresa.

Con el lanzamiento del Service Management Institute SMI® nace la nueva Certificación Profesional en el Ámbito de la Dirección de Servicios, que tiene como objetivo acreditar a los mejores profesionales en dirección de servicios a nivel internacional. Por tanto, es una acreditación global que no depende de sectores o países, sino que es aplicable a cualquier empresa y sector.

El presidente del Consejo Asesor del Service Management Institute SMI®, Marlon Molina, fue el encargado de dar la bienvenida al acto de lanzamiento, que calificó como "un momento histórico", ya que "casi 20 años después pasamos a atender la dirección y la gestión de todos los servicios en un mundo 'As a Service'".

"El sector público y el sector privado, todos están viviendo una gran transformación. Hasta el año 2030 vamos a movernos de los productos a un mundo 'As a service', un mundo absolutamente lleno de servicios que, además, interactúan unos con otros. Hace 20 años que ya existe la profesión de gestión de servicios y hoy ha nacido oficialmente la Asociación de Director de Servicios. Tenemos una gran oportunidad porque todo está por crear, pero desde nace desde la experiencia", resaltó Molina.

CONTINÚA EN PRÓXIMA PÁGINA

Acto seguido, el presidente del Service Management Institute SMI®, Javier Peris, apuntó que la presentación es "el renacimiento" de itSMF España, que a partir de ahora aplicará su conocimiento en dirección servicios no únicamente a IT, sino a todos los departamentos: "La asociación lleva 20 años en los que ha ido aprendiendo, los servicios han ido cambiando, las tecnologías han ido apareciendo, hemos vivido nuevos enfoques y tecnologías, y de alguna manera cada vez más vamos a un mundo más 'As a Service' donde no solo se requieren gestión de servicios sino verdaderos Directores de Servicios" .

Por tanto, "si lo que la ciudadanía necesita es percibir los servicios, también deberíamos de acreditar a verdaderos directores de servicios que los ofrezcan con el valor que se espera", recalcó el presidente de Service Management Institute SMI®. De esta forma, nace esta comunidad global que tiene como objetivo certificar a aquellos profesionales que cuentan con las habilidades necesarias para no solo gestionar sino tambien dirigir servicios.

En este punto, Javier Peris destacó que a pesar de que "estamos impactados por una cantidad de servicios tremenda, hasta la fecha se le había dado demasiada importancia al proyecto". "Los proyectos son necesarios, pero tienen una fecha de inicio y de fin conocida, mientras que los servicios son lo que perdura, se disfruta y el usuario de verdad percibe. Es fácil encontrar disciplinas, metodologías y profesionales formados y certificados como directores de proyectos, pero hasta hoy no era fácil encontrar profesionales en dirección de servicios. Gracias al Service Management Institute ya es posible, podemos encontrar la alta dirección formada adecuadamente como Directores de Servicios", añadió.

CONTINÚA EN PRÓXIMA PÁGINA

Durante el acto, el presidente del Colegio Oficial de Ingeniería Informática de la Comunitat Valenciana (COIICV), Alejandro Blasco, se congratuló de que la asociación escogiera la Semana Informática como el espacio idóneo para presentarse de forma oficial y consideró "muy oportuno el momento de nacimiento de Service Management Institute SMI®", que representa a un colectivo que tiene mucho que ver con la parte IT, pero que va más allá.

A continuación, tuvo lugar un acto simbólico sobre el escenario de Las Naves, con una fotografía de familia de representantes de los cuatro sectores 'padrinos' de Service Management Institute SMI®: Manuel Serrat, Vicepresidente de la Asociación de Técnicos Informáticos de la Administración Local ATIAL; a Carlos Pampliega, Vicepresidente del Capítulo de Madrid del Project Management Institute PMI Madrid; Cayetano Hernández, Presidente de la Federación de Asociaciones de Informática de la Salud FAIS, y Alejandro Blasco, presidente del Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana COIICV.

Tras la fotografía, la presidenta del Consejo Académico del Service Management Institute SMI®, Esperanza Marcos, presentó la Base de Conocimiento de la Asociación, el Service Management Body of Knowledge SMBoK®, quien afirmó que "estamos en un mundo absolutamente de servicios". La globalización, el aumento de la esperanza de vida o la transformación digital son algunos de los factores que, según Esperanza Marcos, han provocado que, cada vez más, las economías se basen en servicios.

En su ponencia, la presidenta del Consejo Académico del Service Management Institute SMI® explicó que, a pesar de estar en un mundo de servicios, las organizaciones trabajan como en una época industrial y los profesionales siguen formándose de esta manera. Por este motivo, señaló, es el momento de empezar a formar a profesionales para un mundo de servicios y para organizaciones de servicios.

"Nos faltan certificaciones de profesionales en dirección de servicios. El Service Management Institute SMI® es una iniciativa muy pertinente en este momento y estamos trabajando en la elaboración de un cuerpo de conocimientos que defina qué conocimientos debe tener un director de servicios", resaltó.

A su juicio, el director de servicios es como el director de orquesta: "No tiene que saber tocar perfectamente el piano o ser un experto violinista, pero necesita saber cómo suena cada instrumento y saber en qué momento y con qué intensidad les tiene que dar la entrada".

CONTINÚA EN PRÓXIMA PÁGINA

Tras la intervención de Esperanza Marcos, fue el turno del Vocal y miembro de la Junta Directiva del Service Management Institute SMI®, Marcos Navarro Alcaraz, quien expuso los detalles de la Certificación Service Management Profesional SMP® y su Proceso de Grandfathering que permite por Méritos Propios obtener la Certificación. Marcos Navarro detalló que, con la creación del Service Management Institute SMI®, se extiende la vinculación anterior de itSMF únicamente con la tecnología, para pasar a acreditar y reconocer además de certificar a profesionales de todos los sectores y ámbitos.
"Queremos que los servicios no solo se gestionen sino se dirijan cada vez mejor, esa dirección va a requerir mejores profesionales y que se puedan identificar más fácilmente. Generando esta certificación lo que queremos es que se puedan identificar de la misma forma que cuando las empresas buscan profesionales en la dirección de proyectos", explicó.
Marcos Navarro subrayó que se trata de una certificación global, que no depende de sectores, países o tecnologías, por lo que es aplicable a cualquier empresa: "Nuestro objetivo primordial con la certificación es que, mirando a una sala, sepamos quienes tienen el pin del Service Management Profesional SMP® del Service Management Institute SMI®. Queremos que sea un distintivo de calidad de los profesionales". Así, el objetivo del Service Management Institute SMI® es generar una certificación que sea reconocida por la industria y que permita evaluar a buenos profesionales en la dirección de los servicios, mediante experiencia, conocimientos y un examen de evaluación.

Por último, Marlon Molina Presidente del Consejo Asesor del Service Management Institute SMI® presentó y moderó la mesa redonda titulada 'La Dirección y Gestión de Servicios en la Administración Pública y la Alta Dirección' con la participación de Inmaculada Sánchez Ramos, de Madrid Digitaliza; Ana Bastida, del Instituto Municipal de Informática del Ayuntamiento de Barcelona; y Ana María Pont, de la Oficina de Proyectos Europeos del Ayuntamiento de Valencia. En dicha mesa, las ponentes abordaron la necesidad de extender la cultura de los servicios a las administraciones públicas, del reto que supone para éstas el mundo 'As a Service' o de la importancia de la figura del director de servicios.

En su intervención, Inmaculada Sánchez insistió en la importancia de "generar ecosistemas de relación y confianza mutua en las administraciones públicas, porque las realidades hoy en día son sofisticadas y son servicios continuos, y no proyectos que empiezan y acaban". "Toda la vida hemos ofrecido servicios, pero el mundo 'As a Service' supone movernos en procesos dinámicos y flexibles, antes éramos muy lineales y ahora estamos en un mundo totalmente dinámico", dijo.

Para Inmaculada Sánchez, las administraciones públicas han de adaptarse al mundo actual y "aprender a pensar fuera de la caja", de forma que se ponga al ciudadano en el centro. También insistió en la necesidad de crear consejos asesores para que se generen espacios de colaboración público-privada.

CONTINÚA EN PRÓXIMA PÁGINA

Institute

Por su parte, Ana Bastida recalcó la importancia de "impulsar servicios y proyectos transversales porque los ciudadanos necesitan que tengamos una visión holística de los mismos y que cuando les ofrezcamos un servicio, lo hagamos de manera transversal".

Sobre el nacimiento de Service Management Institute SMI®, Bastida lo calificó como "una oportunidad" para trasladar el concepto de gestión y de dirección de servicios no al ámbito de IT, sino al ámbito municipal y de todas las administraciones públicas. "Espero y deseo que esta iniciativa ayude a las administraciones públicas a posicionarse como administraciones 'As a Service', que es lo que esperan los ciudadanos: tener una administración líquida en consonancia con lo que es la sociedad actual", aseguró.

Respecto a este cambio hacia el mundo 'As a Service' en las administraciones, Ana Pont consideró que es "un camino que todavía no hemos explorado y que puede ser parte de la solución a este estado de bienestar en el que vivimos y que queremos fortalecer". Para ello, resaltó que "el proceso de transformación en las administraciones públicas debe partir desde arriba: desde la visión política hacia abajo".

En este sentido, Ana Pont señaló que "es un reto y una obligación" transformar cómo funcionamos en las administraciones y extender la cultura del proyecto a la dirección de servicios. "Es más necesario que nunca el Service Management Institute SMI® sobre todo para las administraciones y los empleados públicos. El mundo gira cada vez más 'As a Service' y los ciudadanos requieren que las administraciones, como prestadoras de servicios, lo hagamos cada vez mejor, con un coste más eficiente y que el ciudadano realmente se sienta satisfecho con lo que hacemos", concluyó.

Un evento el Lanzamiento del Service Management Institute SMI® que concluyó con un vino español, cóctel y exhibición de corte y degustación de Jamón ibérico a cargo de un maestro cortador que permitió el Networking y el intercambio de experiencias, anécdotas y conocimientos entre distinguidos profesionales tanto del sector público como el privado llegados tanto de distintos puntos de la geografía española como de países donde el Service Management Institute SMI® empieza a tener presencia.

ABOGADOAMIGO

Bufete Experto en
Nuevas Tecnologías

NUEVOS MASTERS

eGob®

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