ESPECIAL

"Hack&News"

DE Tecnología & Sentido Común

AGOSTO 2022

Seguridad en nuestros archivos: EL CIFRADO 08

¡Los firewalls llegan a la nube! 12

CÓMO PERDER 7.000M EN 6 HORAS 16

Tendencias en ciberseguridad 2022 20

Ahora la guerra se libra en internet 28

32 La respuesta ante incidentes de seguridad, asignatura pendiente.

36 Bug hunters: Los cazadores

40 Ciberataque a Iberdrola

44 Pegasus,el software de "moda"

48 Radar COVID APP: La historia.

safecreative
2 010025 512318
INFO ABOUT RIGHTS

“ESPECIAL Hack&News”

DE Tecnología & Sentido Común

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

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

GABINETE JURÍDICO
Jesús López Peláz

ATENCIÓN AL LECTOR
tecnologiaysentidocomun@businessandcompany.com

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

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

safeCreative
2 010025 512318
INFO ABOUT RIGHTS

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

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

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

ALBERTO RODRÍGUEZ

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

LinkedIn: https://www.linkedin.com/in/a-rodriguezp/

Twitter: https://twitter.com/albert0r

27-28 SEPTIEMBRE | VIRTUAL | GRATUITO

DIGITALIZE AND AUTOMATE

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

5000 PARTICIPANTES

25 PONENTES, LÍDERES Y EXPERTOS DIGITALES

1 INVITADO SORPESA

2 DÍAS DE CONTENIDO EXCLUSIVO

INNOVACIONES TECNOLÓGICAS

CASOS DE ÉXITO

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

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

efecte

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

REGÍSTRATE

Premios recibidos

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

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

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

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

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

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

Pasos firmes

Comprueba cómo los estándares ayudan a tu empresa

www.pasosfirmes.es

UNE
Normalización Española

Asociación Española de Normalización
une@une.org - www.une.org -

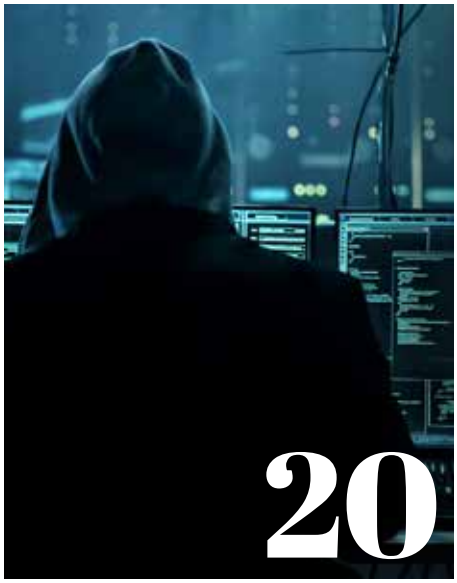
Organismo de normalización español en

ISO IEC CEN CENELEC ETSI COPANT

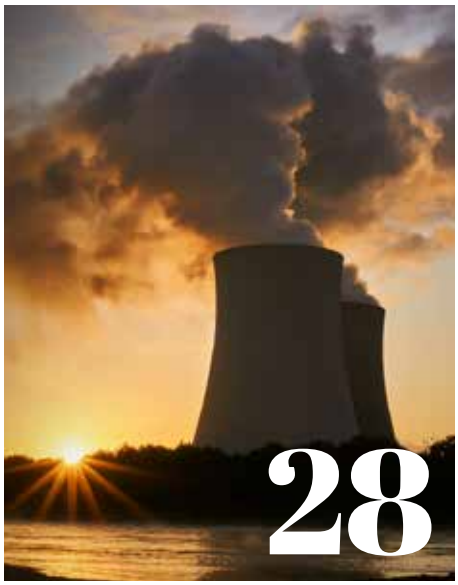
ESPECIAL AGOSTO 2022

índice
DE CONTENIDOS

https://tecnologiaysentidocomun.com



Tendencias en ciberseguridad 2022



Ahora la guerra se libra en internet

Bug hunters: Los cazadores

Radar COVID APP: La historia.

Índice de Contenidos

Índice de Contenidos 06

Seguridad en nuestros archivos: El cifrado 08

¡Los firewalls llegan a la nube! 12

Cómo perder 7.000M en 6 horas 16

Tendencias en ciberseguridad 2022 20

Vuelven los eventos presenciales de ciberseguridad 24

Ahora la guerra se libra en internet 28

La respuesta ante incidentes de seguridad, asignatura pendiente. 32

Bug hunters: Los cazadores 36

Ciberataque a Iberdrola 40

Pegasus,el software de “moda” 44

Radar COVID APP: La historia. 48

índice

#TYSC

Seguridad en nuestros archivos: El cifrado

El cifrado, en informática, no es más que convertir datos con un formato totalmente legible, a datos que sólo se pueden leer o procesar después de un descifrado.

Este tipo de herramienta es fundamental para impedir que alguien lea o sustraiga información de un sistema informático con fines maliciosos. Esta herramienta se utiliza tanto por parte de grandes compañías como por usuarios individuales con la única finalidad de proteger información.
Otras de las ventajas que ofrece el cifrado es presentarse como un medio para demostrar tanto la autenticidad como el origen de la información, junto con la posibilidad de verificar el origen de un mensaje y confirmar que no ha sido modificado durante la transmisión del mismo.
Para entender el cifrado, es importante tener claros los conceptos de cifrado y claves. Cuando se envía la información, ésta se cifra mediante un algoritmo y se descifra mediante la clave apropiada. Esta clave se puede, o bien almacenar en el sistema de recepción, o bien, transmitirse junto con los datos cifrados.

Los métodos para cifrar y descifrar la información van evolucionando a medida que los métodos de captura y robo de esta información cifrada van cambiando y adaptándose a cada momento. Estos métodos pueden incluir o cifrados con clave simétrica o criptografía asimétrica.

En el cifrado de clave simétrica, también conocido como algoritmo de clave secreta, la clave de descodificación de mensajes ha de ser provista al receptor antes de que el mensaje se pueda descodificar. La clave que se usa en la codificación es la misma que se utiliza en la descodificación, lo que resulta más conveniente para los usuarios individuales y los sistemas cerrados. De lo contrario, se le tiene que enviar la clave al receptor, lo que aumenta el riesgo de alteraciones en caso de que terceros, como un atacante malicioso, la intercepte. La ventaja es que este método es mucho más ágil que el método asimétrico.

CONTINÚA EN PRÓXIMA PÁGINA

En la criptografía asimétrica, se utilizan dos claves diferentes (pública y privada), que están vinculadas entre sí matemáticamente. Las claves son solo números extensos vinculados entre sí, pero no son idénticos, de ahí el término asimétrico. La clave pública se puede compartir con cualquier persona, mientras que la clave privada debe mantenerse en secreto. Ambas se pueden usar para cifrar un mensaje, y la clave opuesta a la que se emplee para cifrarlo se utiliza luego para descodificarlo.

Uno de los errores más comunes que cometemos es proteger mal la clave de cifrado. Es muy importante tener una clave robusta para que los archivos se cifren bien y que no se vean comprometidos durante un ataque. La mayoría de los programas suelen ofrecernos como medida de seguridad un fichero de recuperación que hemos de guardar en un lugar seguro, ya que sin él perderíamos el acceso a la información cifrada. Por desgracia, muchos usuarios toman la decisión errónea de guardar ese fichero de recuperación junto al resto de ficheros cifrados, lo cual hace totalmente inútil el cifrado de la información.

En sistemas operativos Windows, contamos con Bitlocker como herramienta nativa para el cifrado de disco. En el caso de que optemos por una alternativa de código abierto, una de las más utilizadas es VeraCrypt.

Hace unos años, algunos países, expresaron su interés por poner puertas traseras al cifrado. Actualmente hay una “batalla” entre defensores y detractores del cifrado, incluso hay una guerra abierta entre diferentes gobiernos por el cifrado existente en algunas aplicaciones que a día de hoy utilizamos en nuestra vida cotidiana, léase WhatsApp, Telegram o Signal.

La batalla ha comenzado, ¿Tú cifras? Yo sí.

Bienvenidos a esta nueva temporada de Tecnología y Sentido Común.

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.

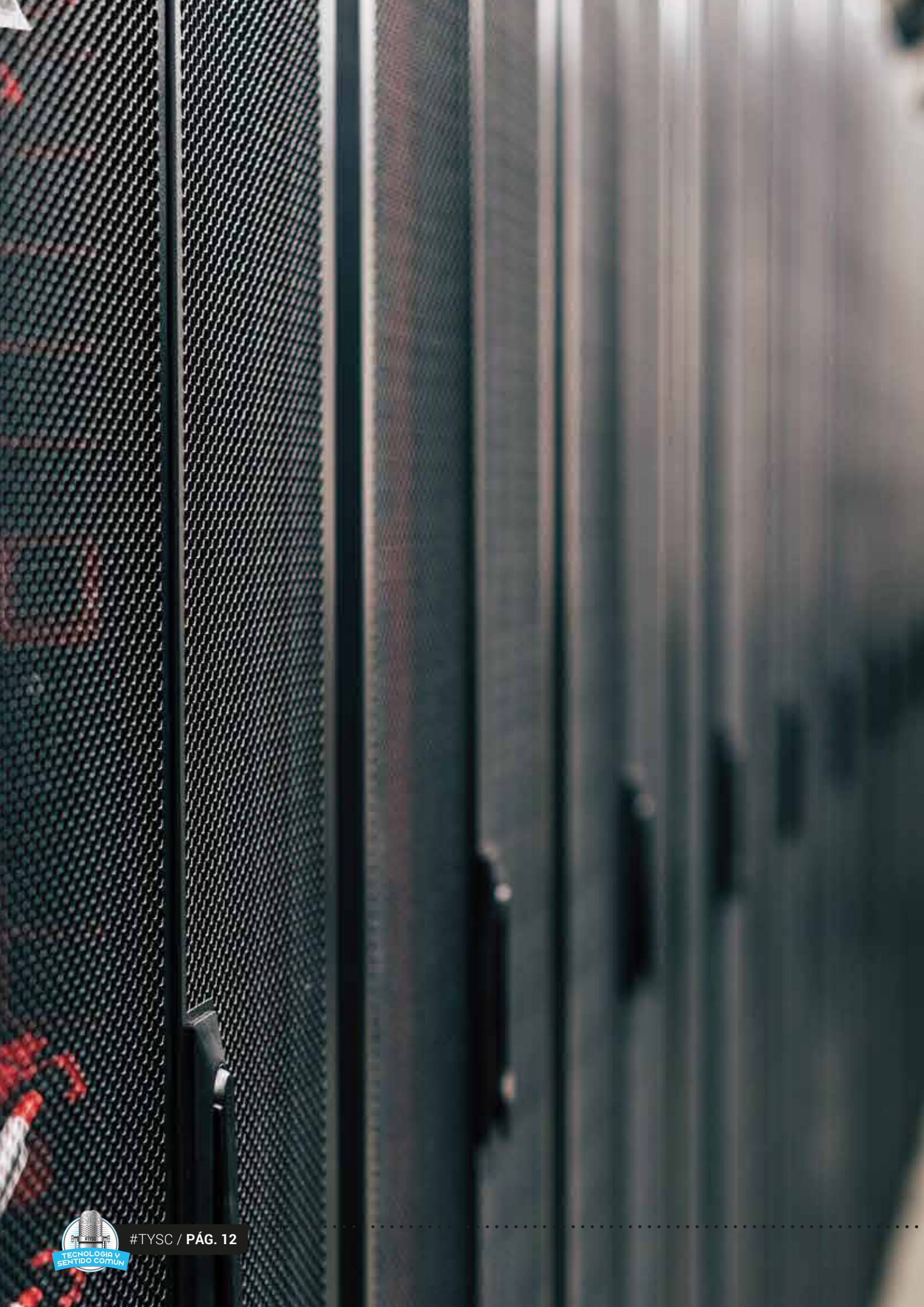
FORMACIÓN BUSINESS CLASS

- 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



¡Los firewalls llegan a la nube!

Durante muchos años, las empresas han administrado sus propios firewalls on-premise o han tenido dispositivos propios en los centros de datos donde se encontraban sus servidores, pero administrados por proveedores externos de servicios. En estos casos el proveedor asume la administración del dispositivo, llegando a su operación e incluso a su política de seguridad en algunos casos, para de esta forma descargar de estas funciones al equipo de IT.

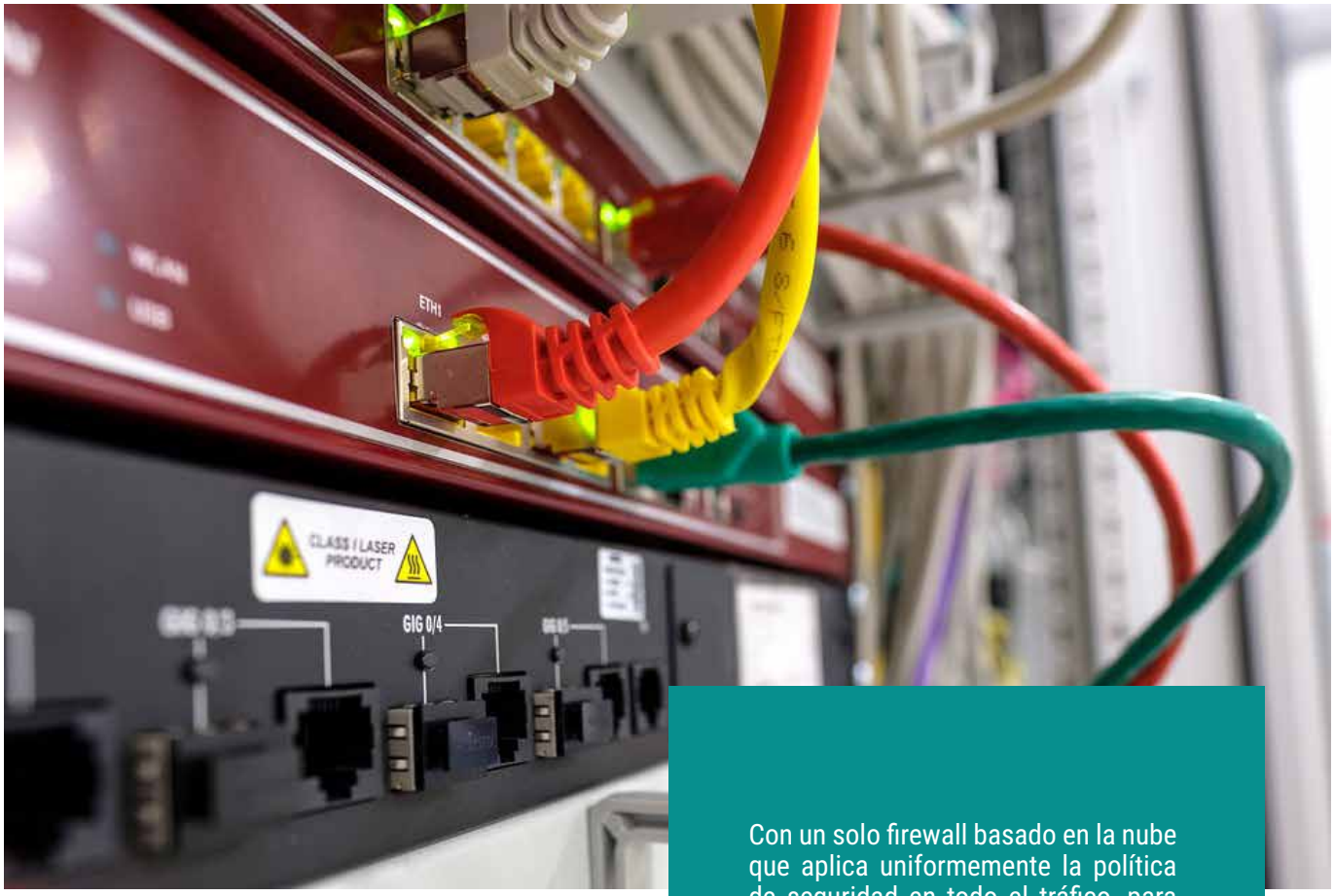
El firewall como servicio propone una nueva arquitectura, una transformación de un factor en forma de dispositivo a un verdadero servicio en la nube.

Pero ¿Qué es FWaaS? En muchos sentidos, FWaaS se parece mucho a un firewall de hardware que tendría en las instalaciones. Sin embargo, tiene distintas ventajas, como por ejemplo la capacidad de escalar casi instantáneamente para adaptarse a una red en expansión.

Todo esto es posible, gracias a que está basado en la nube. Por lo tanto, se puede moldear de acuerdo con el tamaño, la configuración, la demanda y las necesidades de seguridad únicas de la compañía que lo implanta.

La propuesta de esta tecnología es proporcionar una arquitectura más simple y más flexible mediante el aprovechamiento de la administración de políticas centralizadas, múltiples funciones de cortafuegos empresariales y túneles de tráfico para mover total o parcialmente la gestión de la seguridad a una infraestructura en la nube.

CONTINÚA EN PRÓXIMA PÁGINA



FWaaS permite a las organizaciones establecer políticas locales seguras para todas las aplicaciones sin necesidad de comprar, implementar o administrar dispositivos de seguridad. Las capacidades de seguridad, incluido el firewall de capa 7 completo, se brindan como un servicio en la nube que escala elásticamente para manejar la inspección SSL, el ancho de banda creciente, las demandas de los usuarios, y el tráfico de aplicaciones en la nube con conexiones de larga duración. La administración centralizada desde una única consola permite a las organizaciones ofrecer una protección idéntica para cualquier usuario, en cualquier dispositivo, donde sea que se conecten, ya sea en la oficina corporativa, visitando una sucursal local o trabajando desde casa.

En entornos en los que varios firewalls conviven la política de seguridad es difícil de gestionar, y esto conlleva un mayor nivel de riesgo.

Con un solo firewall basado en la nube que aplica uniformemente la política de seguridad en todo el tráfico, para todas las ubicaciones y usuarios este problema se minimiza y simplifica, reduciéndose de forma considerable el nivel de riesgo y homogeneizándose.

Hace unos años, la mayor parte de compañías optaban por mantener sus cortafuegos dentro de sus propias instalaciones. Estos firewalls se diseñaron hace bastante más de una década y en su diseño no se planteó el poder admitir aplicaciones en la nube. Tiene todo el sentido del mundo que a medida que las aplicaciones se trasladan a la nube estos dispositivos hagan lo mismo.

¿Piensa que es una buena solución para tu compañía? ¡En unos años hablamos!

MGEIT® MPPM® eGob®

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

CERTIFÍCATE EN PROCESOS

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

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

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

Nivel de Certificación Executive*

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

Nivel de Certificación Leader*

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

Nivel de Certificación Skilled*

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

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

MISION

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

FORMACIÓN BUSINESS CLASS

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

CONVOCATORIAS 2022/23

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

eGob

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

Cómo perder 7.000M en 6 horas

A principios del mes de octubre volvían a saltar las alarmas, ¡Facebook no funciona!, ¡Instagram tampoco! ¡Ni WhatsApp! Todo el mundo se preguntaba qué estaba ocurriendo, más de 3000M de usuarios afectados y los tres grandes… desaparecidos de internet.

Pero ¿Qué llevó a estos tres gigantes a desaparecer de la red? La respuesta ya la conocemos, una configuración técnica errónea en su protocolo BGP (Border Gate Protocol). Muchos de vosotros, habréis escuchado durante estos días a técnicos y expertos hacer mención a este protocolo. Pero, ¿Qué es BGP y cómo funciona? El protocolo BGP es un mecanismo para intercambiar información de enrutado entre los denominados sistemas autónomos (AS).

Aquí es donde entra a jugar una definición de internet que todos conocemos desde hace años. Internet es una red de redes, que utiliza grandes routers, en los que hay una gran cantidad de listas de las posibles rutas que puede usar un paquete para llegar a su destino. Es el protocolo BGP el que indica a las demás redes que está disponible.

CONTINÚA EN PRÓXIMA PÁGINA

TikTok
ouTube

Cada una de estas redes tiene lo que se denomina ASN (Autonomous System Number) que no es más que una red individual con una serie de normas de enrutamiento de paquetes. Los ASN van indicando sus rutas a través del BGP para interconexionar redes entre sí.

Tanto Facebook, como Instagram y WhatsApp dejaron de anunciar sus rutas a los prefijos de sus servidores de DNS. Ellos solitos se borraron de internet.

Este error provocó picos de peticiones a sitios como Twitter y aplicaciones de comunicación, como puede ser el caso de Signal o Telegram, que también produjo algunos episodios de lentitud en las mismas.

¿Cuáles son los principales daños que este problema ha ocasionado? Tras algo más de seis horas de caída, las acciones Facebook cayeron en torno a un 4,89% de su cotización en bolsa, únicamente en bolsa se perdieron en torno a los 7.000 millones de dólares. El impacto a nivel de usuarios afectados no se queda atrás, más de 3000 millones, por no hablar del daño reputacional sufrido.

Aunque a muchos les parezca demasiado tiempo de caída hemos de destacar la importancia que tiene un buen plan de continuidad de negocio. Las pérdidas han sido muy elevadas y tener un buen RTO (Recovery Time Objective) en estos casos es de vital importancia para la compañía. Personalmente 6 horas no me parece excesivo, pero si nos fijamos en la coste-efectividad, vemos claramente que hay que acelerar los procesos de recuperación del servicio/negocio.

Otro de los casos importantes para analizar que nos ha ofrecido este mes de octubre es la caída del servicio de OVH. Tras el incendio de uno de sus centros el pasado marzo, esta caída está achacada a un "error humano". Durante la actualización de su sistema anti DDoS se produjo un error de configuración en uno de sus routers que provocó un fallo de la red. Aunque el error quedó corregido en aproximadamente una hora, la caída de la infraestructura de OVH ha supuesto una cantidad de pérdidas que presuponemos elevada, debido a la cantidad de empresas y usuarios que utilizan este proveedor de servicios.

Al día de cierre de esta editorial aún no se ha cuantificado dicha cantidad.

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

Tendencias en ciberseguridad 2022

El año 2021 va a ser recordado como uno de los años históricos en el número de ciberataques registrados, pero ¿Qué nos depara el año que está por llegar?

Teniendo en cuenta las características de ataques recibidos durante este año que está a punto de finalizar, durante el próximo 2022 deberemos de prestar atención a *viejos conocidos* que volverán con bastante más fuerza.

Las ***noticias falsas y campañas de desinformación*** servirán de trampolín para que los ciberdelincuentes lleven a cabo sus ataques y estafas. A lo largo de 2021, se difundió información errónea sobre la pandemia de la COVID-19 y la correspondiente vacunación, creemos que este tipo de campañas seguirán muy activas durante 2022 y que se utilizarán ganchos más sofisticados.

Al igual que al finalizar 2020 hacíamos especial foco de atención sobre las ***filtraciones de datos***, este año 2022 nos hace pensar que se producirán a una mayor escala y con un mayor impacto, ocasionando un coste más elevado, tanto para gobiernos como para empresas, ya que la recuperación será bastante más costosa.

El ***ransomware*** será otro de los ataques que pensamos que durante 2022 tendrá más impacto. Se prevé que el precio de los rescates exigidos por los ciberdelincuentes aumente de forma considerable. Durante el año 2021, a nivel mundial se calcula que 1 de cada 61 empresas experimenta un ransomware a la semana. Toda aquella compañía que pueda permitirse pagar un rescate por su información está claramente en la zona de peligro.

CONTINÚA EN PRÓXIMA PÁGINA

Los ***dispositivos móviles*** volverán a estar en el punto de mira, a medida que el pago electrónico y el uso de dispositivos móviles para el mismo se vaya extendiendo, los ciberdelincuentes evolucionarán y adaptarán sus técnicas de ataque para de esta forma explotar la dependencia de los dispositivos móviles que hemos ido adquiriendo.

Los ***servicios en la nube*** creemos que tampoco pasarán desapercibidos para los malos y aprovecharán las vulnerabilidades encontradas en los mismos para lanzar ataques a gran escala contra el cloud.

Hay un dicho popular, que reza tal que *"poderoso caballero es don dinero…"* y en 2022 lo seguirá siendo. Las ***criptomonedas*** y los wallets, seguirán siendo objetivo de los ciberdelincuentes. Allá por agosto de 2021 vimos como se produjo el mayor robo de criptomonedas de la historia, que llegó a los 600M de dólares. La ciberseguridad es importante y más que necesaria para protegerse de atacantes que roba todo tipo de criptomonedas.

Para terminar con estas tendencias para 2022, tenemos que hablar de la ***ciberguerra***. Durante los últimos años hemos venido viendo como la guerra se ha desplazado a la red y hemos escuchado a un número muy elevado de analistas que apuntan que la III Guerra Mundial se está librando en el ciberespacio. Este hecho lleva a pensar que durante el próximo año se producirá un incremento en el número de ciberataques entre países, con el único objetivo de desestabilizar todo tipo de actividades a nivel mundial.

Personalmente, y como vengo haciendo desde hace bastante tiempo, creo que la inversión en materia de ciberseguridad debe crecer bastante más de lo que lo ha hecho y que es el punto de inflexión para poder contener lo que se nos viene encima este año 2022.

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

Vuelven los eventos presenciales de ciberseguridad

Tras más de año y medio de eventos virtuales o de los denominados "híbridos", el equipo de RootedCON ha llevado a cabo, este pasado mes de diciembre, su primera edición de RootedCON Málaga en la ciudad andaluza. El evento ha sido el primero 100% presencial desde la aparición de la COVID 19, y se han tomado las medidas de seguridad necesarias para cumplir la normativa sanitaria vigente en Andalucía.
La gente tenía ganas de volver a coincidir en este tipo de eventos, y hasta la capital de la Costa del Sol acudieron más de 300 personas de diversos lugares de España, Barcelona, Galicia, Comunidad Valenciana, Madrid… quedando en lista de espera, debido al aforo, más de 150 personas.

RootedCON planteó en Málaga, un evento similar en estructura al que realizan en Valencia, con un día dedicado a las formaciones y otro a las charlas. Durante el día de las formaciones se ofreció un amplio abanico de posibilidades que abarcaba desde Hardware Hacking sobre IoT, a Exploiting, Hacking Ético o caza de malware, de mano de profesionales de reconocido prestigio como Jesús Muñoz, Pablo San Emeterio, Pablo González o Roberto Amado.

CONTINÚA EN PRÓXIMA PÁGINA

El día de las charlas empezó con una Keynote de la mano del Alcalde de Málaga, Francisco de la Torre, que dio la bienvenida a todos los asistentes y volvió a dejar patente su apuesta por Málaga como uno de los hubs de ciberseguridad más preparados a nivel europeo. Por su compromiso con la tecnología y la ciberseguridad, fue galardonado con el premio Antonio Ropero, dotado con 2.500€, que el alcalde ha donado íntegramente a Cáritas.

En RootedCON hay una visión más allá de la seguridad, y cualquier tema relacionado con la tecnología o cultura tecnológica tiene cabida. La primera de las charlas no era ni más ni menos que una charla sobre la historia del Theremin, con un mini concierto incluido, de la mano de Javier Díez-Ena, que encandiló a los asistentes. La mañana venía fuerte, cargada de esteganografía de la mano de Nicolás Moral para continuar con la espectacular charla de Alfonso Muñoz, una de las principales eminencias que tenemos en criptografía. Durante los descansos, reencuentros con amigos y muchísimo networking. Se respiraba de nuevo ambiente de CON.

Tras la comida, el talento local hizo su aparición de la mano de Sergio de los Santos y una charla sobre malware. Las redes era otro de los puntos a tocar y Blanca Fernández de Córdoba nos lo recordó con su charla "El Doctor Strange quiere gestionar tu infraestructura". La guinda del pastel, la pondría Abraham Pasamar, con una impresionante charla sobre reversing y explicación de diferentes técnicas.

Había asistentes de todo tipo, estudiantes, profesionales, C levels, y esto hizo que todos saliéramos de allí bastante más enriquecidos de lo que llegamos y con un montón de ideas locas a las que poder darle una vuelta al llegar a casa.
Por desgracia, no se pudo llevar a cabo, por prudencia, la habitual fiesta que se organiza después de un evento de RootedCON, pero esto no desmereció el evento, del cual los organizadores sacan una valoración muy positiva.

Ya se está trabajando en la próxima edición de RootedCON en Madrid, el mes de marzo de 2022 y que traerá muchas sorpresas.

¡Larga vida a los eventos presenciales!

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

Ahora la guerra se libra en internet

Esta frase es una de las más escuchadas, leídas y escritas de los últimos tiempos. La guerra tiene un nuevo campo de batalla, la red. Cuando hablamos de Rusia, China, Irán, Corea del Norte, hablamos de grandes potencias y no solamente potencias militares. Estos países tienen un verdadero arsenal en lo que a herramientas para poder efectuar ciberataques se refiere, y un verdadero "ejército" de personas que realizan este tipo de ataques. Pero empecemos por el principio.

¿Qué es la ciberguerra? La ciberguerra o guerra tecnológica es todo aquello referente al uso de ataques digitales por parte de un país para dañar los sistemas informáticos más esenciales de otro país. El objetivo es encontrar vulnerabilidades tecnológicas en los sistemas informáticos del "enemigo" para obtener datos, información sensible o simplemente para dañarlos y destruir servicios esenciales.

El lanzar un ciberataque a los sistemas informáticos de una infraestructura crítica conlleva un grave daño a la misma y a los servicios que presta. La bolsa, medios de transporte, instalaciones de abastecimiento, agua, electricidad, son algunos de los escenarios que más riesgo presentan de ser objetivos en un hipotético caso de ciberguerra.

En España, es el CNPIC (Centro Nacional de Protección de Infraestructuras Críticas y Ciberseguridad) el máximo responsable de proteger dichas infraestructuras y de las políticas de ciberseguridad del Ministerio de Interior. Impulsa, coordina y supervisa todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas.

CONTINÚA EN PRÓXIMA PÁGINA

Todos recordamos Stuxnet, primer gusano conocido que espía y reprograma sistemas industriales, en concreto sistemas SCADA de control y monitorización de procesos, que podía afectar a infraestructuras críticas como centrales nucleares. Irán fue el país más afectado por este gusano, y se especuló que el objetivo de este era atacar a infraestructuras de “alto valor” en ese país, incluyendo centrales nucleares como Bushehr o el complejo nuclear de Natanz. Nunca se tuvo “claro” el origen de ese ciberataque, pero conocemos sus consecuencias, tomó el control de 1.000 máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse. Fue la primera vez que un ataque cibernético logró dañar una infraestructura del "mundo real".

Pero ¿Qué más objetivos puede tener una ciberguerra? Los sabotajes como el que hemos mencionado anteriormente con Stuxnet son uno de los principales objetivos, pudiendo dar lugar a interrupciones de servicios o a daños más graves.

Otro de los principales objetivos de la ciberguerra es la propaganda. Tener el control de la información con la correspondiente influencia en la opinión pública es un tipo de ciberguerra psicológica que se consigue basándose en campañas de desinformación en redes sociales, medios digitales y utilizando para ello las ya más que conocidas “fake news”.

Hemos de tener en cuenta que juegan un papel muy importante los actores “no estatales”. El hecho de que equipos coordinados puedan causar un impacto tan elevado en la geopolítica mundial nos hace plantearnos la gravedad de la ciberguerra y sus consecuencias.

El ciberespacio, es el nuevo lugar donde se van a librar batallas muy pero que muy duras.

MGEIT®

eGob®

CSX + ISO 27000
Information Security
Seguridad de la Información

CERTIFÍCATE EN SEGURIDAD

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

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

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

Nivel de Certificación Executive*

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

Nivel de Certificación Leader*

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

Nivel de Certificación Skilled*

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

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

MISION

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

FORMACIÓN BUSINESS CLASS

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

CONVOCATORIAS 2022/23

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

eGob®

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

La respuesta ante incidentes de seguridad, asignatura pendiente.

Todos sabemos la importancia que tiene una buena respuesta ante un incidente de seguridad en una compañía. Una de las asignaturas pendientes de las pequeñas y medianas empresas es esta. No se gestiona bien dicha respuesta. Pero ¿Qué es la respuesta a un incidente de ciberseguridad?

La respuesta a incidentes es un conjunto de instrucciones que ayudan al personal de IT a detectar, responder y recuperarse de incidentes de seguridad, tanto en sus redes como en sus servicios. Esta respuesta, deben ofrecerla equipos especializados en seguridad junto al resto de equipos de tecnologías de la información que componen la empresa.

Dicha gestión está formada por diferentes etapas, que parten de una preparación, y que aparte de ser la primera etapa, es la clave para que los diferentes equipos puedan ofrecer una respuesta efectiva a cada uno de los incidentes que puedan plantearse.

En esta etapa la empresa debe de desarrollar y documentar políticas de respuesta ante incidentes, y definir las pautas de comunicación. En definitiva, establecer una base sobre la cual poder empezar a trabajar el incidente.

La detección es la segunda de las etapas, en ella se revisan los eventos de seguridad utilizando las herramientas de las que dispone la empresa, se detecta y se alerta del incidente. Para esta etapa es habitual el uso de correladores de alertas dentro de una solución SIEM.

CONTINÚA EN PRÓXIMA PÁGINA

Una vez detectado el incidente se debe contener e intentar neutralizar el mismo. Esta etapa es probablemente una de las más complejas y críticas dentro del DFIR, ya que implica en la mayor parte de los casos, el apagar servicios, limpiar, reconstruir y mitigar las posibles amenazas detectadas previamente. La erradicación del incidente va a ser fundamental para que las operaciones vuelvan a funcionar con normalidad, para ello se ha de encontrar la causa raíz del mismo y realizar las tareas necesarias para proceder a la solución del mismo.Una vez resuelto el incidente, aún queda mucho trabajo por hacer. Se debe documentar cualquier tipo de información o solución que pueda usarse para que eventos similares no se vuelvan a reproducir en el futuro. Completar un informe, monitorizar después del incidente o identificar nuevas posibles medidas preventivas son buenas prácticas en durante todo el proceso de gestión.

Este es, a muy grandes rasgos, el proceso de gestión de incidentes de seguridad. Las grandes empresas lo tienen perfectamente definido y muy bien interiorizado, ya que son conscientes de la importancia que tiene una posible caída de la operación o de la prestación de servicios a terceros, pero ¿Qué pasa con las pequeñas y medianas empresas? Aquí este tipo de procedimientos, o medios, no están tan implantados como en las grandes compañías y ese es uno de los principales vectores que los ciberdelincuentes utilizan para efectuar ataques. Una empresa pequeña no tiende a considerarse propiamente un objetivo de ataque. Es por esto que los daños que se causan en este tipo de empresas son bastante más graves que los que puedan generarse en una empresa con todos los procedimientos de gestión y respuesta a incidentes bien definidos e implantados. El 60% de estas empresas atacadas se ven obligadas a cerrar debido a los daños que una mala gestión de un incidente de seguridad ocasiona.

Todos somos objetivos de ataques y todos tenemos la misma importancia, una buena respuesta a incidentes es fundamental para mantener todas las operaciones a pleno rendimiento tras un ciberataque.

MGEIT®

eGob®

CBCI + ISO 22301
Business Continuity
Continuidad del Negocio

CERTIFÍCATE EN CONTINUIDAD

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

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

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

Nivel de Certificación Executive*

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

Nivel de Certificación Leader*

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

Nivel de Certificación Skilled*

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

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

MISION

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

FORMACIÓN BUSINESS CLASS

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

CONVOCATORIAS 2022/23

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

eGob®

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

Securit

Bug hunters: Los cazadores

¿Qué es un bug hunter? Los bugs hunters son hackers éticos o investigadores que reportan vulnerabilidades a las organizaciones a cambio de una recompensa de tipo económico. Para ello se amparan en programas que tienen como propósito premiar a aquellas personas que logren encontrar fallos y vulnerabilidades en las diferentes soluciones de software, hardware, página web etc de una compañía. Por supuesto hay cumplir una serie de requisitos, como demostrar la vulnerabilidad, explotarla, documentarla, y no difundirla hasta que esté solucionado por completo.

Cumpliendo todos los requisitos, y enmarcados en uno de estos programas tendremos derecho a una recompensa.

Allá por el año 95 Netscape lanzó el primer programa de bug bounty que ofrecía recompensas en efectivo a aquellos que encontraban errores de seguridad en su navegador Netscape Navigator 2.0 Beta. Matt Horner, vicepresidente de marketing de Netscape, explicó en su momento que «al recompensar a los usuarios por identificar y reportar rápidamente errores, este programa fomenta una revisión extensa y abierta de Netscape Navigator 2.0 y nos ayuda a continuar creando productos de la más alta calidad». Fueron pioneros.

CONTINÚA EN PRÓXIMA PÁGINA

Existen empresas que se dedican 100 % a intermediar entre hackers y clientes, utilizando el potencial de la comunidad hacker. Estas son reconocidas como empresas de bug bounty.

Esta historia de intermediarios, recompensas y crowdsourcing está creciendo y depende mucho del nivel de madurez de cada mercado y país. Seguirá creciendo y este tipo de empresas cada vez serán más populares, han logrado democratizar el acceso al servicio de ethical hacking a un precio mucho menor y con el mismo nivel de calidad.

Por el lado del mercado, cada vez más empresas confían y han legitimado este tipo de servicio.

Durante el pasado mes de marzo tuvo lugar, dentro del evento RootedCON, la "Hacker Night". Durante diez horas, una cincuentena de cazadores de bugs se reunió para atacar sistemas informáticos de varias empresas del IBEX35, y otras importantes empresas de fuera de España.

Para acceder al evento, fue necesario aceptar una clausula de confidencialidad y se creo un entorno controlado y totalmente monitorizado para proporcionar seguridad a las empresas participantes.

El premio: 500.000€ en recompensas, la mayor hasta el momento en nuestro país. Este monto era el total a repartir entre los bugs reportados, que se pagan en base al tipo de vulnerabilidad y a la criticidad de la misma.

La noche acabó con más de 20.000€ repartidos entre los researchers que participaron y reportaron vulnerabilidades dentro de las plataformas preparadas para tal efecto. A eso se sumaron 3.000€ que RootedCON otorgó al mejor de los bugs encontrados.

Los programas de bounties, poco a poco, se van afianzando, el tipo de modelo gusta a las empresas y a los investigadores. Es un paso adelante para que este modelo de negocio permanezca y crezca.

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

delete
enter
return
shift
option
esc

Ciberataque a Iberdrola

Era inicio del pasado mes de abril, cuando Iberdrola publicó que a mediados del mes de marzo de 2022 fue víctima de un ciberataque que comprometió los datos de 1,3M de clientes de la compañía.

Los datos comprometidos, según indica la compañía, fueron nombre, apellidos, DNI, domicilio, número de teléfono y dirección de correo electrónico. Desde Iberdrola apuntan a que ningún dato de tipo económico ni de la facturación se han visto comprometidos.

El ataque lo sufrió la filial I-DE Redes Eléctricas Inteligentes, lo que se conocía como Iberdrola distribución. De hecho, es esta filial la que, en cumplimiento del RGPD está contactando con sus clientes para informarles sobre este ataque.

El origen de este, en el momento del cierre de esta editorial, no ha sido revelado, pero se empieza a vincular a una campaña de ataques relacionados con la guerra ucraniano-rusa dirigidos a grandes corporaciones e instituciones públicas españolas como RENFE o el propio Congreso de los Diputados, que experimentaron diversos ataques el mismo día del incidente.

Tras la correspondiente denuncia, interpuesta ante la Brigada Central de Investigación Tecnológica de la Policía Nacional, la compañía realizó la pertinente notificación ante la Agencia Española de Protección de Datos.

CONTINÚA EN PRÓXIMA PÁGINA

La inteligencia española investiga si los grupos de ciberdelincuentes que reciben apoyo del gobierno de Rusia están detrás de esta ofensiva contra empresas e instituciones españolas, ya que al menos uno de los ataques, el perpetrado contra el Congreso de los Diputados, pasó por equipos ubicados en Siberia. El CCN-CERT advirtió que este tipo de ataques podría intensificarse contra países orientales durante las próximas semanas debido a la actual situación geopolítica.

Las principales sospechas, a día de hoy, recaen sobre grupos de ciberdelincuentes de origen ruso pagados por el Kremlin. Suenan los nombres de viejos conocidos como APT28 también conocido como Fancy Bear, que actúan contra occidente desde aproximadamente el año 2014, fecha en la que la invasión de Crimea desató la tensión entre Rusia y la OTAN. Este grupo está directamente relacionado con la unidad militar 26.165 del Centro Principal de Servicios Especiales (GTsSS), un grupo élite de "*descifradores*" nacido en la Guerra Fría y ahora dedicado a coordinar a los ciberdelincuentes.

El segundo grupo se denomina Sandworm Team y es, según los documentos difundidos por el CNI, «un grupo de amenazas destructivas», vinculado a otra unidad del GRU, la 74.455.

¿De qué forma puede afectarnos esto? Es muy importante no bajar la guardia. Seguramente durante las próximas semanas, tal y como desde Iberdrola han comunicado a sus clientes, se deberá de extremar la precaución antes correos electrónicos o mensajes SMS que no cuenten con una identificación clara del remitente, ante posibles ataques de *phishing*. También se aconseja, en caso de observar alguna incidencia, contactar con nuestro operador de telefonía móvil. Entendemos que esta última recomendación se basa en posibles ataques de *SIM Swapping* ya que los números de teléfono de los clientes se han visto comprometidos.

Como comentábamos en nuestro artículo del mes de febrero de 2002, este ataque es un claro ejemplo de que ahora la guerra se libra más que nunca en internet.

¡No bajéis la guardia!

MGEIT®

eGob®

DAMA + ISO 38505
Data Governance
Gobierno del Dato

CERTIFÍCATE EN
GOBIERNO DEL DATO

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

NIVELES DE CERTIFICACIÓN

Nivel de Certificación Board*

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

Nivel de Certificación Executive*

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

Nivel de Certificación Leader*

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

Nivel de Certificación Skilled*

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

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

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

eGob®

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

Pegasus, el software de “moda”

Durante estas últimas semanas, hemos leído y escuchado hablar mucho sobre Pegasus y la verdad es que, a raíz de la salida a la luz de algunas informaciones, daría para escribir varias novelas de espionaje dignas del mismísimo Ian Flemming. Pero ¿Qué es Pegasus? Pegasus es un software desarrollado por la empresa israelí NSO Group cuya función principal era investigar delitos por parte del crimen organizado o el terrorismo.

La venta de este software, hasta donde nosotros sabemos, está regularizada por el ministerio de defensa de Israel, que en teoría se encarga de cerciorarse que todas las ventas de este software son correctas y que únicamente se vende a gobiernos y fuerzas y cuerpos de seguridad.

Hasta aquí todo más o menos correcto. El problema viene cuando salen a la luz noticias que podrían evidenciar que NSO Group habría vendido este software fuera de los “clientes permitidos”.

Pero ¿Cómo funciona Pegasus? Se trata de un software que se aprovecha de las vulnerabilidades de los teléfonos para de esta forma obtener la información. Para ello, compra en el mercado negro vulnerabilidades, por ejemplo, de whatsapp, que es una aplicación de uso muy extendido, o incluso de la calculadora. Aplicaciones que prácticamente todos tenemos en nuestros dispositivos y cuyas vulnerabilidades podrían hacer de “puente” para acceder al mismo.

CONTINÚA EN PRÓXIMA PÁGINA

La venta de este software se hace por licenciamiento. Una licencia, un intento de intrusión. Si ese intento es fructífero se conseguiría el acceso total al dispositivo. En caso de fallo de ese intento el comprador habría gastado una licencia.

En un estado de derecho, como el existente es España, ningún organismo puede hacer uso de este software sin previa autorización judicial y para intervenir un teléfono se ha de argumentar ante un juez, de forma muy clara, los motivos existentes para dicha intervención.

Hemos de dejar claro que este software puede usarse en otros países fuera de España e infectar un dispositivo en nuestro territorio.

Pegasus registra prácticamente todo, puede utilizar la cámara o puede leer mensajes cifrados, de modo que cuando estás infectado puedes pasar incluso a ser un "altavoz" de absolutamente toda tu vida, ya que también puede activar de forma remota el micrófono del dispositivo.

Tanto Apple como Facebook han presentado sendas demandas contra NSO Group. Apple incluso ha facilitado información sobre la herramienta Forcedentry, también de NSO Group y que podría ser capaz de colar el spyware en dispositivos Apple a víctimas concretas.

Apple bloqueó los mecanismos que se utilizaban para entrar indebidamente en los iPhone mediante su actualización a iOS15, es por esto por lo que en su día se insistió en la actualización a esta versión.

Estamos en un momento en el que la vigilancia y contravigilancia están a la orden del día, herramientas como Pegasus pueden cuestionar las prácticas, más o menos éticas, de los gobiernos que adquieren o han adquirido este tipo de herramientas.
La polémica está servida. ¿Seguridad? ¿Privacidad? ¿Ambas? ¿Ninguna?

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

Radar COVID APP: La historia.

Allá por el mes de agosto de 2020 se empezó a hablar de una aplicación de rastreo de personas contagiadas por la COVID19. Esta APP nació de manos de la Secretaría de Estado de Digitalización e Inteligencia Artificial, la aplicación utilizaba una api de rastreo de contactos creada por Google y Apple para que las aplicaciones oficiales de cada gobierno pudieran aprovecharla para rastrear contactos sin tener que crearlo todo desde cero. Se intentaba automatizar el trabajo de los rastreadores. El sistema estaba basado en tecnología Bluetooth, cuando la aplicación estaba instalada y activa, el móvil **generaba una clave aleatoria diaria** a partir de la cual se generan identificadores que cambian pasados entre 10 y 20 minutos y se transmiten a los móviles cercanos mediante esta tecnología. Este código aleatorio se emitía varias veces por segundo usando el Bluetooth del móvil y los móviles cercanos que tenían también Radar Covid instalado lo recogían, de modo que ambos móviles registraban el contacto.

Una buena idea, en una situación complicada, no exenta de polémica ya que, desde abril de 2020, el equipo técnico y de desarrollo estaba al tanto de vulnerabilidades en materia de protección de datos, según consta en un documento técnico publicado durante el mes de abril de 2020. La AEPD, indica que "registró varias reclamaciones en las que se denunciaba una vulnerabilidad en el diseño de la aplicación", que permitía, por ejemplo, asociar una IP con la subida de un test positivo, lo que excedía lo necesario para cumplir sus funciones y permitía desanonimizar la información, vulnerando así la última versión de la política de privacidad de la propia app.

CONTINÚA EN PRÓXIMA PÁGINA

¿Por qué estamos hablando de esto? La respuesta es sencilla. Durante el mes de Junio de 2022 la Agencia Española de Protección de Datos (AEPD) publicó un expediente sancionador contra la Secretaría de Estado de Digitalización e Inteligencia Artificial, que fue el organismo que firmó el contrato con la empresa encargada del desarrollo y mantenimiento de la aplicación. En dicho expediente, la AEPD establece que la Secretaría de Estado de Digitalización reconoció que "para el proyecto piloto no se generó ningún documento de evaluación de impacto de protección de datos". Ante esto, sólo puedo decir, olé, olé y olé

La Ley Orgánica 3/2018, de 6 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, que entre otros aspectos adapta a nuestra normativa el RGPD, no contempla multas cuando el incumplimiento es obra de una administración pública: el expediente se saldará con un mero apercibimiento, sin penalización económica.

Al respecto únicamente diré que es la ley y que por supuesto hay que cumplirla. ¿Es justo esto? Desde mi punto de vista no, no lo es. Todos los que trabajamos en tecnología en empresas privadas, todos los que gestionamos proyectos en empresas privadas, todos los que gestionamos servicios en empresas privadas, somos conscientes de que un error de este tipo tiene unas consecuencias muy graves. En mayo de 2022 Google fue multado con 10M de euros por ceder datos a terceros sin estar legitimado para ello y por obstaculizar el derecho de supresión de los ciudadanos.

¿Por qué no se depuran responsabilidades en la administración pública? ¿Por qué no se penaliza económicamente a los responsables?

El uso de Radar COVID fue un fracaso, un coste final de en torno a 4M de euros y los datos de miles de sus usuarios al descubierto.
Este parece que será un verano más normal que los dos últimos, estimados lectores, os deseo unas ¡felices vacaciones!

IFEMA MADRID

Llámalo ingenio.
Llámalo IFEMA MADRID

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

ifema.es

Siente la inspiración

NUEVOS MASTERS

eGob®

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