Identi :: SiC

Ser... para creer

Madrid | Hotel Novotel Campo de las Naciones

15 y 16 de noviembre_2023

Organiza:

Revista SiC

www.revistasic.com/identisic

Copatrocinan:

Delinea · ForgeRock · okta · Omada · pwc · SailPoint · WatchGuard

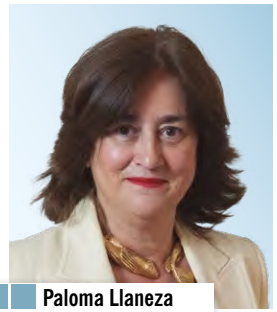
Identidad, atributos y tecnologías: fiarse en la justa medida

La confianza en la esfera digital de la sociedad tiene una cuenta pendiente con el concepto de identidad, el establecimiento de los datos en los que esta se sustantiva, la validez de los atributos, la fortaleza de las credenciales, las capacidades de hacer y deshacer a efectos legales y el entramado en el que deben ir operando los proveedores de servicios de confianza en lo que atañe a la integración de la privacidad y la ciberseguridad por diseño y en el ciclo de vida de la actividad, su evaluación y certificación.

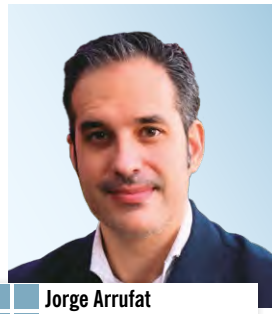
En la UE (con el eIDAS2 al caer y el desarrollo de las carteras digitales en marcha) se ha entendido la problemática existente hasta ahora como un freno a las relaciones comerciales en el espacio interior. Por tanto, su respuesta se enfoca a favorecer el desarrollo del mercado europeo. Sin embargo, algunos estados miembros valoran también la identidad digital como un asunto de soberanía nacional.

Por otra parte, los sistemas de IAM/CIAM –orientados a entornos intraempresariales, multinacionales y extendidos– han experimentado un extraordinario avance tecnológico y funcional en todos los entornos, modos de servicio y subprocesos específicos: identificación, autenticación, autorización, control de accesos, trazabilidad y auditoría, brindando herramientas ágiles, escalables y adaptables a las necesidades de las organizaciones.

El programa de esta edición de IdentiSIC ofrece una perspectiva de ambos mundos y de los caminos abiertos para que confluyan.

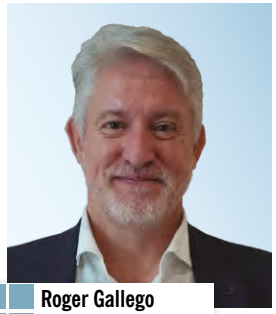


Paloma Llaneza
RAZONA LEGALTECH



Jorge Arrufat
BBVA NEXT TECHNOLOGIES

Julio Castilla
PwC ESPAÑA



Roger Gallego
DELINEA

PROGRAMA

15 de noviembre. 2023

09:00h. Acreditación

09:30h. **eIDAS2, carteras de identidad digital y PSC cualificados ante la encrucijada de su certificación y supervisión en la UE**
Paloma Llaneza
CEO. **RAZONA LEGALTECH**
Directora Técnica del Esquema eIDAS & eIDE en **CerteIDAS**

09:55h. Coloquio

10:00h. **FIDO (Fast IDentity Online): logros y futuro de la estandarización de tecnologías para autenticación de usuarios en un mercado global**
Jorge Arrufat
CISO. **BBVA Next Technologies**

10:25h. Coloquio

SERVICIOS

10:30h. **ITDR: evolucionando la gestión de amenazas IAM**
Julio Castilla
Director Identity & Data Governance. BSS.
PwC España

10:55h. Coloquio

11:00h. Pausa-café

SOLUCIONES Y TECNOLOGÍAS

11:30h. **DELINEA**
Roger Gallego
Iberia Sales Manager

11:55h. **FORGEROCK**
Carlos Scott
Consultor de Riesgo Digital

12:20h. **OKTA**
Nuno Silveiro
Large Enterprise Account Executive

12:45h. Coloquio con los participantes

13:30h. Almuerzo para todos los asistentes

Fin de la 1ª sesión

Carlos Scott
FORGEROCK

Nuno Silveiro
OKTA

Jorge Dávila
UPM

Ignacio Alamillo
LOGALTY

16 de noviembre. 2023

09:00h. Acreditación

09:30h. **La Identidad Digital ante el requisito de la ciberseguridad y la privacidad por diseño y los sistemas de IA**
Jorge Dávila
Consultor Independiente
Director del Laboratorio de Criptografía LSIIS
Facultad de Informática
UNIV. POLITÉCNICA DE MADRID

09:55h. Coloquio

10:00h. **Consideraciones ante una eventual futura Ley española de identificación digital**
Ignacio Alamillo
Advisor. **LOGALTY**

10:25h. Coloquio

SERVICIOS Y EXPERIENCIAS

10:30h. **Gestión segura de 'identidades' y accesos de cosas en entornos OT/IoT**
Vicente Segura
Gerente de Producto de Ciberseguridad OT&IoT
TELEFÓNICA TECH

10:55h. Coloquio

11:00h. Pausa-café

SOLUCIONES Y TECNOLOGÍAS

11:30h. **OMADA**
Jorge Sendra
Country Manager Iberia

11:55h. **SAILPOINT**
Alejandro Fernández
Solutions Engineer

12:20h. **WATCHGUARD**
Miguel Carrero
Vice President, Managed Security Service Providers & Strategic Accounts

12:45h. Coloquio con los participantes

13:30h. Almuerzo para los asistentes

Fin de la 2ª sesión y del evento

Vicente Segura
TELEFÓNICA TECH

Jorge Sendra
OMADA

Alejandro Fernández
SAILPOINT

Miguel Carrero
WATCHGUARD

* Revista SIC se reserva el derecho a modificar el contenido o los ponentes de este programa si las circunstancias así lo requieren.

PAM

IaM

Autenticación

Autorización

IA

Protección de Credenciales

eIDAS2

Identidad descentralizada

CiaM

Iniciativas como eIDAS2, FIDO2, así como la 'explosión' de identidades no humanas y los multiversos marcarán la actualidad en 2023

Credenciales seguras, legales y fáciles de para ser y hacer en la sociedad conecta

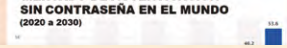
Revista SIC repasa en este especial, previo al VIII Congreso IdentiSIC, el 16 y 17, en Madrid pasando con la identidad digital y su protección en nuestro ciberuniverso, así como sus gra en 2023, un año que vendrá marcado por la popularización de los sistemas 'sin contraseña' de Apple, Microsoft y Google, a través de FIDO2, así como la llegada del eIDAS2 con el que se una identidad digital útil a cada europeo, que dispondrá de una cartera (*wallet*) digital pa todo tipo de trámites. Eso sin olvidarse de la 'meta'-identic multiversos y sus avatares, los cuales influirán también en nue de relacionarnos y hacer negocios al más puro estilo 'Ready P y donde la identidad será el gran pilar que garantice su éxito más allá de la Web 3.0.

ANA ADEVA Y JOSÉ MANUEL VERA (Equipo SIC)

GOOGLE, APPLE y MICROSOFT, junto con FIDO, dan un paso de gigante para un mundo sin contraseñas

El **Foro Económico Mundial** (**WEF**) publicó en 2020 un documento titulado 'Autenticación sin contraseña: el próximo avance en la transformación digital segura', abogando por un "futuro sin contraseñas". En él, explicaba que alrededor del 80% de los ciberataques sufridos en ese año estaban relacionados con contraseñas. Y es que estas se basan en el conocimiento, lo que significa que se pueden adivinar o robar fácilmente. Por eso, una de las grandes tendencias para 2023, según muchos analistas, será la, por ticamente a sus credenciales de inicio de sesión de FIDO en muchos de sus dispositivos, siempre que sean de una marca similar, sin tener que volver a inscribir cada cuenta. Ahora, Apple ya ofrece este sistema en su iOS16 y Google lo hará en Android y el navegador Chrome antes de que finalice el año. Entre sus ventajas destaca porque una *'passkey'* no puede reusarse en otros sitios o *apps*, no puede filtrarse en una brecha de seguridad y protege al usuario frente a los ataques de *phishing*. Al cierre de esta edición,

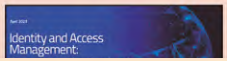
MERCADO DE AUTENTICACIÓN SIN CONTRASEÑA EN EL MUNDO
(2020 a 2030)



Entre sus principales obstáculos figuran el *Shadow* IT, la experiencia de usuario y el posible freno al negocio, según un estudio de CRA

Los sistemas IAM, en modo local, nube o híbrido, ganan peso en las empresas a pesar de la reticencia de los usuarios y la falta de presupuesto

Se espera que el mercado global de gestión de accesos e identidades registre



zado en enero de este año y con la participación de más de 200 profesionales de ciberprotección de EE.UU., su objetivo era saber serio la necesidad de avanzar en este ámbito", dice el estudio que, también, explica que resulta "fascinante" las diferentes formas

Los fondos de capital riesgo apuestan por las empresas de protección de la identidad como uno de los mercados de mayor proyección

Debido al incremento de la complejidad de la superficie de ataque y del entorno que proteger, la gestión de identidades y accesos (IAM), así como la administración de los accesos y la identidad de los clientes (CIAM) están comenzando a superponerse e integrarse con otras herramientas, como el inicio de sesión único (SSO), el gobierno de la identidad (IGA), la gestión de accesos privilegiados (PAM) o la gestión de identidades de máquinas y cargas de trabajo en la nube, una situación que ha hecho que todo este mercado esté en expansión.

de 12.000 millones en un solo año para ser uno de los grandes gigantes mundiales en este campo.

También, ha sido significativo que la propia **Ping Identity** pusiera en marcha un fondo de capital riesgo, **Ping Ventures**, para financiar "nuevos negocios centrados en la protección ante el fraude en línea, la verificación de identidad en tiempo real y el gobierno de identidad". Su primera inversión la ha realizado en la compañía de autenticación y control de acceso unificado, **Allthenticate.**

Crecimiento constante

Así, según datos de **Markets and Markets,** el merca-

Principales compañías en identidad y gestión de accesos

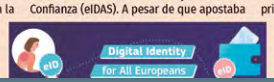
eIDAS2: el gran impulso a las billeteras digitales para los ciudadanos

Se espera que este próximo año se apruebe **eIDAS2**. Se trata de una actualización de la regulación que establece que todos los países de la UE deben poder proporcionar una billetera digital a cualquier ciudadano que quiera usar versiones digitales de documentos de identidad clave. El requisito es parte de un impulso más amplio para la transformación digital en la UE, en la medida en que el gobierno quiere facilitar al máximo el acceso de las personas a diversos servicios en línea.

Digital ID, Europa podría ser una de las primeras regiones del globo en adoptar el uso de billeteras digitales a escala comercial.

Se trata de la culminación de un proceso que comenzó en 2014 cuando la UE presentó la primera versión del Reglamento de la UE sobre Identificación Electrónica y Servicios de Confianza (eIDAS). A pesar de que apostaba

un valor equivalente entre el 3% y el 13% d PIB para 2030. Con su puesta en marcha, l usuarios podrán almacenar formas electr nicas de identificación y otros document oficiales (carnet de conducir, recetas, dipl mas, etc.) de forma segura. Esta informaci será proporcionada únicamente por fuent privadas confiables. Los usuarios podrán d cidir cuántos datos quieren compar para un propósito específico y cualqu... ciudadano o empresa de la UE tendrá la capacidad de probar su identidad o cual-



El galimatías de los estándares de identidad

La identidad digital y el mercado de gestión de acceso y control viven sometidos a la tensión que supone la coexistencia de múltiples estándares y enfoques que buscan un equilibrio adecuado entre utilidad, privacidad y seguridad. Así, se pueden encontrar desde marcos de confianza –que crean preocupaciones transfronterizas y desafíos de interoperabilidad entre proveedores de servicios públicos y privados a nivel nacional–, hasta tecnologías como las PKI (para una gestión de la identidad centralizada) o *blockchain* (para una identidad descentralizada). De hecho, muchos caciones excesivamente regionales.

Por ello, organismos como **Enisa** han realizado varios estudios en profundidad sobre la identidad digital, comenzando por definirla de forma precisa como "una representación única cia recuerda la amplia variedad de organismos que trabajan en desarrollar estándares de identidad: desde los europeos como **ETSI, CEN** y **CENELEC,** hasta internacionales de normalización como **ISO, ITU, IEEE, IEC, Common Criteria, ICAO** e, incluso, consorcios como **IETF, CA/ Browser Forum, CSC, OASIS, OpenID** y **FIDO,** además de organismos públicos nacionales como el **ANSSI** francés, el **BSI** alemán, el **BSI** británico o **NIST** en EE.UU.

Además, el organismo ha realizado varias recomendaciones, en este ámbito, para poner en marcha una estandarización de identidad digital en Europa ple-

Trazabilidad

Zero Trust

Biometría

EU ID Wallet

Cadena de Bloques

Sin contacto

Robo de Identidad

Robotización

Aprovisionar

IdentiSIC

- ¿Qué efectos tendrá en la gestión de identidades la integración de sistemas de IA en entornos heterogéneos (personas y cosas) altamente automatizados?
- ¿Por qué sendas tecnológicas están avanzando los desarrolladores de soluciones para todos o cada uno de los procesos para realizar una gestión segura de identidades y accesos?
- ¿En qué medida los actuales entornos de nube y … As a Service están potenciando la necesidad de disponer de soluciones PAM (Privileged Access Management) para fortalecer los controles de acceso a activos privilegiados?

- ¿Qué papel está jugando FIDO Alliance en el avance de la incorporación de tecnologías estandarizadas para la autenticación de usuarios?
- ¿Cómo están abordando las compañías especializadas en ciberseguridad la antifragilidad y la usabilidad de los sistemas de IAM/CIAM?
- ¿Qué requisitos legales deben cumplir los tratamientos de datos en los que estén integrados sistemas biométricos, sistemas biométricos multimodales, sistemas pseudo biométricos y sistemas de reconocimiento de pautas asistidos por IA, orientados a la autenticación de usuarios?

LUGAR Y FECHAS

15 y 16 de noviembre de 2023
Hotel Novotel Campo de las Naciones.
C/ Amsterdam, 3. 28042 Madrid

ORGANIZA

Revista SIC. Ediciones CODA.
C/ Goya, 39. 28001 Madrid
Tel.: 91 575 83 24
info@revistasic.com / www.revistasic.com

SOLICITUD DE INSCRIPCIÓN GRATUITA

El procedimiento para la solicitud de la inscripción es vía web mediante la cumplimentación de un formulario. El aforo será limitado y se fijará en función de las medidas sanitarias vigentes.

Una vez realizada la solicitud, la organización le confirmará su inscripción. En base a qué tipo de asistencia se haya solicitado (presencial o en remoto), se le indicará la forma de proceder.

Sitio web: **www.revistasic.com/identisic**

FORMATO MIXTO: **presencial y retransmitido**

Los datos personales que se solicitan, cuya finalidad es la formalización y seguimiento de su solicitud de inscripción y/o asistencia a IdentiSIC, serán objeto de tratamiento por Ediciones Coda. Usted puede ejercitar sus derechos, reconocidos en la legislación vigente española y del resto de la UE sobre Protección de Datos de Carácter Personal (acceso, rectificación, supresión, limitación, oposición y, si aplicara al caso, portabilidad), en el domicilio del responsable del fichero: Ediciones Coda, S.L., C/ Goya, 39, 2ª planta. 28001 MADRID