



Identi::sic

Un desafío global
ante la transformación

LA IDENTIDAD DIGITAL SEGURA
EN LA SOCIEDAD CONECTADA
INTELIGENTE

Organiza:

Revista **Sic**

www.revistasic.com/identisic

Madrid_
29 y 30 de octubre_2019

Hotel Novotel Campo de las Naciones

Copatrocinan:

 **BeyondTrust**

 **CYBERARK**


Building a better
working world

 **MICRO
FOCUS**

 **okta**

 **pwc**

 **SailPoint**

 **thycotic**

 **transmit**
SECURITY

 **víntegris**
SEGURIDAD DE LA INFORMACIÓN

De la transformación de la IaM + CiaM a la construcción de la IDoT

Cada minuto que pasa se nos van perfilando con mayor nitidez los componentes del universo digital: nube, OT, IoT, 5G, agentes de IA, automatización robótica de procesos, explotación inteligente del dato... Y sea cual sea el entorno al que nos estemos refiriendo (intraorganizativo y extendido –empleados y proveedores–, B2B, B2C, B2A, C2C...), hay una persistente coincidencia de los analistas: la necesidad de alcanzar un consenso sobre la concepción de las identidades de personas y entidades, su gestión segura y la de los accesos a recursos, y el establecimiento de los límites del anonimato como elementos esenciales para una sociedad transformada en la que haya seguridad jurídica.

En esta edición de IdentiSIC se tratarán diversos asuntos del máximo interés al respecto, como son el papel de la identidad en las nuevas operativas bancarias, la gestión de la identidad de las cosas (IDoT), la identidad digital SSI y descentralizada, los nuevos enfoques para el emprendimiento de proyectos de modernización de los sistemas empresariales de IaM/CiaM, el fortalecimiento de la gestión de riesgos de seguridad en los accesos privilegiados (algo que debería estar hoy en la agenda de prioridades de todos los CISOs) y la propuesta de alternativas tecnológicas de última generación para el soporte a la IaM/CiaM y sus subprocesos.



Juan Francisco Losa
BBVA



Nelson Sánchez Vera
EY



Andrés Diego Hontiveros
PwC



Jorge López Ranz
BeyondTrust



Anastasia Sotelsek
CyberArk

PROGRAMA

29 de octubre. 2019

09:00h. Acreditación

09:30h. **El tratamiento de la identidad en las arquitecturas de las nuevas operativas bancarias**

Juan Francisco Losa

Global TISO (Technology Information Security Officer)

BBVA

10:00h. Coloquio

SERVICIOS

10:05h. **EY**

Nelson Sánchez Vera

Spain & MED Identity and Access Management Leader

10:30h. **PwC**

Andrés Diego Hontiveros

Socio Responsable de Identidad y Gobierno del Dato
Business Security Solutions

SOLUCIONES Y TECNOLOGÍAS

10:55h. **BeyondTrust**

Jorge López Ranz

Territory Sales Manager

11:20h. Pausa-café

11:50h. **CyberArk**

Anastasia Sotelsek

Principal Sales Engineer

12:15h. **Micro Focus**

Jacinto Grijalba

Cybersecurity Sales Manager

12:40h. **Okta**

Juan Per Muñoz

Channel Sales Manager. Spain and Italy

13:05h. Coloquio con los participantes

14:00h. Almuerzo para los asistentes



Jacinto Grijalba
Micro Focus



Juan Per Muñoz
Okta



Jorge Dávila
UPM



Nacho Alamillo
Astrea



Pablo Gómez
Generalitat de Catalunya

30 de octubre. 2019

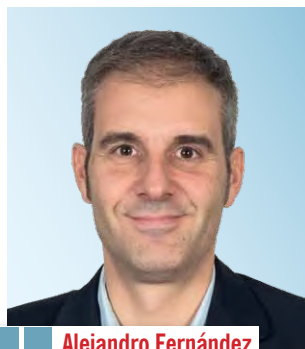
- 09:00h. Acreditación
- 09:30h. **El antagonismo entre la identidad y el anonimato**
Jorge Dávila
Director del Laboratorio de Criptografía
Universidad Politécnica de Madrid
- 09:55h. Coloquio
- 10:00h. **IdentiCAT, el proyecto de identidad digital SSI de Cataluña**
Nacho Alamillo
Director. **Astrea**
Pablo Gómez
Gestor Técnico de la Secretaría de Políticas Digitales y Administración Pública
Generalitat de Catalunya
- 10:25h. Coloquio
- 10:30h. **La gestión de la identidad de las cosas - IDoT**
Javier Hidalgo
Arquitecto de Soluciones del Sector Industrial
GMV eSecure Solutions
- 10:55h. Coloquio

SOLUCIONES Y TECNOLOGÍAS

- 11:00h. **Sailpoint**
Alejandro Fernández
Ingeniero preventa
- 11:25h. Pausa-café
- 11:55h. **Thycotic**
Sergio Marín
Enterprise Sales South Europe
- 12:20h. **Transmit Security**
Javier Jarava
Principal Solution Engineer
- 12:45h. **Vintegris**
Alberto Guidotti
CEO
- 13:10h. Coloquio con los participantes
- 14:00h. Almuerzo para los asistentes



Javier Hidalgo
GMV eSecure Solutions



Alejandro Fernández
Sailpoint



Sergio Marín
Thycotic



Javier Jarava
Transmit Security



Alberto Guidotti
Vintegris

Identidad de confianza

Gartner prevé que, en sólo tres años, el 40% de las empresas apostará por la 'identidad digital como servicio' frente al 5% actual

La autenticación biométrica abanderará el control de las identidades y los accesos a la red corporativa a través de las aplicaciones en el móvil

La evolución de las estrategias de ciberseguridad hacia la protección del dato, especialmente, cómo y quién accede a él, está haciendo que las soluciones y servicios de gestión de identidades y accesos (IAM) vayan ganando terreno dentro de las empresas. De hecho, la firma analista Gartner estima que este mercado puede llegar a alcanzar cerca de los 12.000 millones de euros en 2022.

A la hora de implementar un proyecto de IAM, la autenticación biométrica proporciona una mejor

las empresas que busquen el uso de los smartphones como tokens deben ser conscientes de que este tipo de tecnologías, que se pueden aplicar fácilmente en cualquier teléfono de última generación, son vulnerables a ataques de spoofing o suplantación de identidad a través de fotos, videos, grabaciones de voz,

Así, la autenticación biométrica o por voz, es una de las tecnologías que se están utilizando para mejorar la seguridad de los sistemas de acceso a la red corporativa.

satisfacer la mayoría de sus necesidades, un incremento exponencial en comparación con tan sólo el 5% que se registró en 2018.

Las principales razones por las que un importante porcentaje de empresas se vaya a decantar por esta modalidad es que los proyectos de IDaaS -Identity as a Service-

disponibilidad en el mercado y la dificultad para encontrar y retener a los profesionales con las habilidades necesarias para implementar y operar software de IAM heredado, está provocando que muchas empresas estén dispuestas a adoptar soluciones de gestión de identidades digitales como servicio.

PAM

Autorización

Aprovisionar

Biometría

Establece cinco características clave: preparación, veracidad, seguridad, disponibilidad y administración

El NIST ayuda a proteger los sistemas de control de acceso estableciendo qué propiedades deben tener sus atributos

El Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU. ha presentado una guía que describe las características básicas que deberían tener los atributos utilizados en los sistemas de control de accesos de las agencias federales y otras organizaciones. La publicación Especial 800-205, titulada 'Attribute Considerations for Access

Para el NIST, la confianza en las decisiones de control de acceso depende de la precisión, integridad y disponibilidad adecuadas de dichos atributos. Por eso recomienda establecer, definir y restringir de acuerdo a unos valores



hay que tener en cuenta en sus diferentes categorías (sujeto, objeto y entorno), dentro de un sistema de control de accesos. Estos son:

1. **Preparación.** Con este concepto, el NIST hace referencia a una adecuada planificación del mecanismo de creación e intercambio de atributos, así como en la definición de reglas para mantener su privacidad en todo momento.

Sólo tres de cada 10 ejecutivos piensan que es un ámbito seguro, según un informe de CyberArk

La falta de claridad sobre quién es responsable de la seguridad en entornos de nube se agrava por la inseguridad del acceso privilegiado

"El 36% de las organizaciones afirma que el principal beneficio de la migración de aplicaciones críticas, datos de clientes y cargas de trabajo a entornos de nube pública es liberarse de la gestión de los riesgos de seguridad", destaca el nuevo estudio de CyberArk, bajo el título "Informe mundial de amenazas avanzadas 2019: enfoque en la nube", realizado entre 1.000 directivos y responsables de TI de Estados Unidos, Reino Unido, Francia, Alemania, Singapur, Israel y Australia. Unos datos que se contraponen con el anterior informe de amenazas que evidenciaba que las empresas intentan reducir el riesgo migrando a la nube y exigiendo protección a sus proveedores.

Entre sus conclusiones más llamativas, destaca que las empresas siguen siendo "demasiado dependientes de los proveedores de nubes

de claridad sobre quién es responsable de la seguridad en la nube se ven agravados por un fallo general en la seguridad del acceso privilegiado en

cipales motivos de preocupación, el más acuciante es el acceso privilegiado a los sistemas de nube.



nocen que existen credenciales, secretos y cuentas privilegiadas

Autenticación

IIoT

CiaM

Trazabilidad

Crea un Equipo de Identidad Digital formado por miembros de instituciones públicas y privadas, como parte de su programa GOV.UK Verify, que ha comenzado su segunda fase

REINO UNIDO pone en marcha un proyecto para usar datos personales 'oficiales' para autenticarse en operaciones financieras

El Gobierno británico ha puesto en marcha un proyecto piloto para ayudar a las organizaciones a verificar la identidad digital de las personas, usando como prueba la información que los ciudadanos utilizan para registrarse en servicios de la Administración como, por ejemplo, los datos del pasaporte.

Se trata de un paso importante, ya que el fraude de identidades en el país ha aumentado en los últimos años y se está convirtiendo en un verdadero problema. El Reino Unido espera que la implementación de este proyecto piloto ayude a reducir el fraude y a mejorar la seguridad de las operaciones financieras.



posee el gobierno sobre los ciudadanos en virtud de esta propuesta. Esto significa que no se compartirán datos personales a menos que el individuo ya los haya proporcionado antes. Por su parte, las empresas participantes en el proyecto recibirán un 'sí' o 'no' respecto a la legitimidad de la información emitida.

El gobierno también afirma que "no existirá una base de datos de identidades central y los ciudadanos serán los que posean el control de sus datos personales".

Con esta iniciativa, el Reino Unido espera que las transacciones en línea sean mucho más seguras.

Robo de Identidad

IaM

Gartner.

Top 10 Security Projects for 2019

1

Privileged Access Management

Top Tips

- PAM projects should at least support multifactor authentication (MFA) for all administrators.
- PAM for third-party access should be a priority.
- Use a risk-based (high, medium, low) approach regarding which accounts to prioritize.

Robotización

DIDS

SSI

Protección de Credenciales

Cadena de Bloques

■ ¿Qué papel le están dando las empresas a la gestión segura de identidades y accesos en las nuevas operativas de negocio digital?

■ ¿Existen soluciones para la gestión de identidades de las cosas (IDoT) y, también, para hacerlo conjuntamente con las identidades de las personas en el universo digital al que nos dirigimos?

■ ¿Qué alternativas ofrece la industria para simplificar y, al tiempo, robustecer, la operativa en el macroproceso de la IaM/CiaM?



■ ¿Se encuentra en la agenda de proyectos urgentes de los responsables de seguridad de la información promover la modernización y fortalecimiento del sistema de gestión de accesos de usuarios privilegiados?

■ ¿Qué tipos de identidades digitales deben convivir —y cómo— en la conjunción de la internet de las personas y la de las cosas para que exista seguridad jurídica?

■ ¿Tienen futuro los sistemas de Identidad Auto-Soberana (SSI) y los basados en identificadores descentralizados (DIDs) en todos los escenarios en los que tiene que operar la identidad digital?

LUGAR Y FECHAS

29 y 30 de octubre de 2019

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. Al ser el aforo limitado, la inscripción se cursará por riguroso orden de fecha de entrada de solicitud.

Sitio web: www.revistasic.com/identisic

- Una vez realizada la solicitud, la organización le informará —por razones de limitación del aforo— si ha quedado inscrito o no.
- En ningún caso se admitirán más de tres inscripciones de profesionales de una misma compañía.

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/ de Goya, 39, 2ª planta. 28001 MADRID