www.sia.es @SIA_es Grupo SIA

DOSSIER DE PRENSA

Publicaciones 2019

Diciembre de 2019

Ábrego consulting

Índice de publicaciones

1. ***BYTE.*** SIA amplía su propuesta de soluciones de continuidad con Everbridge. 7 Febrero 2019
2. ***IT CIO.*** *SIA amplía su propuesta de soluciones de continuidad con Everbridge.* 11 Febrero 2019
3. ***TECHWEEK.*** SIA amplía su propuesta de soluciones de continuidad con Everbridge.11 Febrero 2019
4. ***EXPANSION. ECONOMIA DIGITAL.*** SIA amplía su cartera de seguridad con la alianza con Everbridge. 12 Febrero 2019
5. ***COMPUTING***. La USC, pionera en utilizar firma cualificada en la nube. 18 Marzo 2019.
6. ***DATA CENTER MARKET*** SIA amplía su propuesta de soluciones de continuidad con Everbridge. 8 Febrero 2019.
7. ***EL ECONOMISTA.*** La USC elige a SIA para convertirse en la primera universidad gallega en utilizar firma cualificada en la nube. 15 Marzo 2019
8. ***DATA CENTER MARKET***. La Universidad de Santiago de Compostela implanta firma cualificada en la nube. 15 Marzo 2019.
9. ***BYTE.*** La Universidad de Santiago elige a SIA para utilizar firma cualificada en la nube. 14 Marzo 2019.
10. ***CIO.*** La Universidade de Santiago de Compostela implanta un sistema de firma digital. 19 Marzo 2019.
11. ***RED SEGURIDAD.*** La USC apuesta por SIA para implantar la firma cualificada en la nube. 18 Marzo 2019.
12. ***TECHWEEK.*** La USC elige a SIA para convertirse en la primera universidad gallega en utilizar firma cualificada en la nube. 22 Marzo 2019.
13. ***LIDERESCOMPUTING2019***. 4 Marzo 2019.
14. ***COMPUTING .*** Mutua Universal adopta el servicio de firma en la nube de SIA. 27 Marzo 2019.
15. ***TECHWEEK.*** Mutua Universal impulsa su transformación digital con el servicio de firma en la nube de SIA. 27 Marzo 2019.

Índice de publicaciones

16. ***INTEREMPRESAS. INFORMATICA Y COMUNICACIONES.*** Mutua Universal impulsa su transformación digital con el servicio de firma en la nube de SIA. 28 Marzo 2019.
17. ***DATA CENTER MARKET.*** Mutua Universal implanta un servicio de firma en la nube con Grupo SIA. 27 Marzo 2019.
18. ***BYTE.*** Mutua Universal apuesta por la firma digital en nube de SIA. 2 Abril 2019.
19. ***EL ECONOMISTA.*** Mutua Universal impulsa su transformación digital con el servicio de firma en la nube de SIA. 4 Abril 2019.
20. ***COMPUTERWORLD.*** Ranking 2019. Marzo 2019.
21. ***SEGURITECNIA.*** SIA amplia su propuesta de continuidad de Negocio con Everbridge. Marzo 2019.
22. ***COMPUTING.*** Grupo SIA incrementa su facturación en un 22% hasta los 57 millones de euros. 12 Abril 2019.
23. ***EXPANSION.*** La facturación de SIA aumentó un 22%. 12 Abril 2019.
24. ***INTEREMPRESAS. INFORMATICA Y COMUNICACIONES.*** Grupo SIA incrementa su facturación en un 22% hasta los 57 millones de euros. 12 Abril 2019.
25. ***BYTE.*** Grupo SIA incrementa su facturación en un 22%. 15 Abril 2019.
26. ***RED SEGURIDAD.*** Grupo SIA crece un 22% en 2018 y factura 57 millones de euros. 17 Abril 2019.
27. ***DATA CENTER MARKET.*** El servicio de Salud de Baleares recurre a SIA para garantizar la seguridad del acceso a sus TI. 2 Mayo 2019.

Índice de publicaciones

28. ***COMPUTING.*** Islas Baleares garantiza la seguridad de su Salud. 3 Mayo 2019.
29. ***TECHWEEK.*** El servicio de Salud de Baleares garantiza con SIA la seguridad en el acceso a sus sistemas de Información. 6 Mayo 2019.
30. ***ITCIO.*** El servicio de Salud de Baleares garantiza con SIA la seguridad en el acceso a sus sistemas de Información. 6 Mayo 2019.
31. ***INTEREMPRESAS. INFORMATICA Y COMUNICACIONES.*** El Servicio de Salud de las Islas Baleares garantiza la seguridad en el acceso a sus sistemas de Información con SIA. 6 Mayo 2019.
32. ***EXPANSION.*** Baleares garantiza la seguridad del servicio de salud. 7 Mayo 2019.
33. ***EL ECONOMISTA.*** El servicio de salud de las Islas Baleares garantiza con SIA la seguridad en el acceso a sus sistemas de información. 16 Mayo 2019.
34. ***RED SEGURIDAD.*** SIA actualiza el sistema de gestión de Identidades del Servicio Balear de Salud. Segundo trimestre 2019.
35. ***CIO.*** El IB-Salut de Baleares agiliza el acceso a los sistemas de información sanitarios. 22 Mayo 2019.
36. ***TECHWEEK.*** Grupo SIA incrementa su facturación un 22% hasta los 57 millones de euros. 22 Abril 2019.
37. ***IT CIO.*** Grupo SIA incrementa su facturación un 22% hasta los 57 millones de euros. 22 Abril 2019.
38. ***SEGURITECNIA.*** Las USC apuesta por SIA para implantar la firma cualificada en la nube. Abril 2019.
39. ***COMPUTING.*** SIA y Comillas ICAI colaboran para fomentar la formación en ciberseguridad. 11 Junio 2019.
40. ***EL ECONOMISTA.*** SIA y Comillas ICAI colaboran para fomentar la formación en ciberseguridad. 11 Junio 2019.

Índice de publicaciones

41. ***BYTE TI.*** SIA y el ICAI fomentan la formación en ciberseguridad. 11 Junio 2019.
42. ***DIARIO INFORMÁTICO.*** SIA y el ICAI fomentan la formación en ciberseguridad. 11 Junio 2019
43. ***EXPANSION.*** Formación de Ciberseguridad de SIA y Comillas ICA. Junio 2019.
44. ***INTEREMPRESAS. INFORMATICA Y COMUNICACIONES*** SIA y Comillas ICAI colaboran para fomentar la formación en ciberseguridad. 14 Junio 2019.
45. ***DIARIO ABIERTO.*** La española SIA colaborará en el Máster en Ciberseguridad de la Universidad de Comillas. 14 Junio 2019.
46. ***DATA CENTER MARKET.*** SIA y Comillas ICAI colaboran para fomentar la formación en ciberseguridad. 13 Junio 2019.
47. ***BI-LATINO.*** SIA y Comillas ICAI colaboran para fomentar la formación en ciberseguridad. 13 Junio 2019.
48. ***CSO. COMPUTERWORLD***. SIA y la Universidad de Comillas se unen para fomentar talento en ciberseguridad. 21 Junio 2019.
49. ***ACTUALIDAD ECONÓMICA***. Quién es quién en la Empresa Española. 2019.
50. ***EL ECONOMISTA.*** Imdea impulsa con SIA el desarrollo de investigación en red. 28 Junio 2019.
51. ***REDES&TELECOM***. Imdea Software y SIA implementan un sistema de monitorización de fibra oscura en REDIMadrid. 28 Junio 2019.
52. ***COMPUTING.*** IMDEA Software impulsa el desarrollo de la investigación en red. 1 Julio 2019

Índice de publicaciones

53. ***INNOVANDO.*** Imdea impulsa con SIA un sistema de monitorización activa de todos sus enlaces de fibra óptica mediante la incorporación a su red de la tecnología ADVA ALMIA. 5 JuLio 2019.
54. ***Director TIC***. La ciberseguridad y la posición relevante de la IA. 9 Septiembre 2019.
55. ***COMPUTING.*** La ciberseguridad y la posición relevante de la IA. 12 Septiembre 2019.
56. ***DATA CENTER MARKET .*** La ciberseguridad y la posición relevante de la IA. 11 Septiembre 2019.
57. ***EL ECONOMISTA.*** La ciberseguridad y la posición relevante de la IA. 17 Septiembre 2019.
58. ***CIO. COMPUTERWORLD.*** El servicio de Salud de Islas Baleares apuesta por la firma centralizada. Octubre 2019.
59. ***EL ECONOMISTA. J***avier Jarauta: "En ciberseguridad, la clave está en prevenir los ataques“. 29 Noviembre 2019.
60. ***INTEREMPRESAS. INFORMATICA Y COMUNICACIONES.*** Entrevista a Javier Jarauta, director de Consultoría de SIA. 2 Diciembre 2019.
61. ***COMPUTING.*** “En ciberseguridad, la clave está en prevenir los ataques”. 11 Diciembre 2019.
62. ***INNOVANDO.*** Entrevista a Javier Jarauta, Director de Consultoría de SIA. 16 Diciembre 2019.
63. ***BYTE.*** El fraude del CEO: cuando los más preparados también caen… 12 Diciembre 2019.
64. ***COMPUTING.*** El fraude del CEO. Los más preparados también caen… 17 Diciembre 2019.
65. ***EL ECONOMISTA .***"En ciberseguridad, la clave está en prevenir los ataques“. 19 Diciembre 2019.

sia 30 años

Índice de publicaciones

66. ***EL ECONOMISTA.*** El fraude del CEO: los más preparados también caen. 23 Diciembre 2019
67. ***EL ECONOMISTA. TRIBUNA.*** El fraude del CEO: los más preparados también caen. Diciembre 2019

SIA amplía su propuesta de soluciones de continuidad con Everbridge

SIA y Everbridge han firmado un acuerdo para ofrecer a las empresas los beneficios de las soluciones unificadas que componen la plataforma de Everbridge.

Con esta nueva alianza, SIA incorpora a su actual oferta de seguridad la plataforma de gestión de eventos críticos de Everbridge, que permite garantizar la seguridad de las personas y edificios de una organización para la continuidad del negocio, y la solución IT-Alerting que posibilita evaluar, mitigar y reducir el impacto de cualquier incidente TI, ofreciendo a sus clientes una solución integral para abordar los desafíos de seguridad y, una vez más, de continuidad del negocio.

SIA incorpora a su actual oferta de seguridad la plataforma de gestión de eventos críticos de Everbridge, que permite garantizar la seguridad de las personas y edificios

Para Everbridge este acuerdo supone contar a partir de ahora con el partner más adecuado en España en términos de Seguridad para proporcionar a sus clientes el valor y el retorno de la inversión de sus soluciones.

Una óptima respuesta a las crisis

Gracias a la tecnología de Everbridge, SIA posibilita con estas aplicaciones automatizar y acelerar la respuesta a las brechas de seguridad para la continuidad del negocio proporcionando el mensaje adecuado a la persona apropiada en el momento oportuno. Por otro lado, IT Alerting permitirá a los equipos de soporte de IT comunicarse de manera fluida y eficiente en los momentos de crisis. Esta mejor planificación de respuesta y comunicación ayudará a los clientes a reducir los tiempos de interrupción de sus sistemas más críticos.

Según Enrique Palomares, director general de SIA, “las organizaciones de IT cada vez son más complejas de administrar y dar soporte. Esto da lugar además a un aumento del volumen de alertas que se generan. Los clientes necesitan simplificar y optimizar la administración de estas alertas y estamos convencidos de que Everbridge es el mejor socio para dar la respuesta más adecuada».

José Manuel Villanueva, director de Everbridge en España y Portugal, apunta “estamos encantados de ampliar nuestro alcance en España y Portugal a través de esta alianza con SIA para ayudar a las organizaciones a responder mejor al rápido aumento de las necesidades críticas de IT. Su sólida base de clientes y capacidades de servicio profesional impulsarán nuestro crecimiento dentro del mercado».

El acuerdo se enmarca dentro de la política de alianzas estratégicas que SIA viene desarrollando desde hace años a través de la firma de convenios de colaboración con líderes tecnológicos a nivel mundial, reforzando así su apuesta por la especialización, la formación continua y el trabajo en un entorno de colaboración, con el fin de adaptar la TI a las necesidades de sus clientes.

SIA amplía su propuesta de soluciones de continuidad con Everbridge

SIA y Everbridge se han asociado para ofrecer a las empresas los beneficios de las soluciones unificadas que componen la plataforma de Everbridge. Esta alianza permitirá a las empresas automatizar y acelerar la respuesta ante eventos críticos y contar con una solución integral para evaluar, mitigar y reducir el impacto de cualquier incidente T

SIA (Sistemas Informáticos Abiertos), proveedor líder de soluciones de seguridad y servicios de administración de TI, y Everbridge, líder mundial en la gestión de eventos críticos y aplicaciones de software de Continuidad de Negocio, han firmado un **acuerdo como socios** para ofrecer a las empresas los beneficios de las soluciones unificadas que componen la plataforma de Everbridge

Con esta nueva alianza, SIA incorpora a su actual oferta de seguridad la **plataforma de gestión de eventos críticos** de Everbridge, que permite garantizar la seguridad de las personas y edificios de una organización para la continuidad del negocio, y la **solución IT-Alerting** que posibilita evaluar, mitigar y reducir el impacto de cualquier incidente TI, ofreciendo a sus clientes una solución integral para abordar los desafíos de seguridad y, una vez más, de continuidad del negocio.

Para Everbridge este acuerdo supone contar a partir de ahora con el***partner* más adecuado en España** en términos de Seguridad para proporcionar a sus clientes el valor y el retorno de la inversión de sus soluciones.

Una óptima respuesta a las crisis

Gracias a la tecnología de Everbridge, SIA posibilita con estas aplicaciones **automatizar y acelerar la respuesta**

a las brechas de seguridad para la continuidad del negocio proporcionando el mensaje adecuado a la persona apropiada en el momento oportuno. Por otro lado, IT Alerting permitirá a los equipos de soporte de IT **comunicarse de manera fluida y eficiente en los momentos de crisis**. Esta mejor planificación de respuesta y comunicación ayudará a los clientes a reducir los tiempos de interrupción de sus sistemas más críticos.

Según **Enrique Palomares**, director general de SIA, *"las organizaciones de IT cada vez son más complejas de administrar y dar soporte. Esto da lugar además a un aumento del volumen de alertas que se generan. Los clientes necesitan simplificar y optimizar la administración de estas alertas y estamos convencidos de que Everbridge es el mejor socio para dar la respuesta más adecuada".*

José Manuel Villanueva, director de Everbridge en España y Portugal, apunta *"estamos encantados de ampliar nuestro alcance en España y Portugal a través de esta alianza con SIA para ayudar a las organizaciones a responder mejor al rápido aumento de las necesidades críticas de IT. Su sólida base de clientes y capacidades de servicio profesional impulsarán nuestro crecimiento dentro del mercado".*

El acuerdo se enmarca dentro de la **política de alianzas estratégicas** que SIA viene desarrollando desde hace años a través de la firma de convenios de colaboración con líderes tecnológicos a nivel mundial, reforzando así su apuesta por la especialización, la formación continua y el trabajo en un entorno de colaboración, con el fin de adaptar la TI a las necesidades de sus clientes.

SIA amplía su propuesta de soluciones de continuidad con Everbridge

SIA y Everbridge se han asociado para ofrecer a las empresas los beneficios de las soluciones unificadas que componen la plataforma de Everbridge. Esta alianza permitirá a las empresas automatizar y acelerar la respuesta ante eventos críticos y contar con una solución integral para evaluar, mitigar y reducir el impacto de cualquier incidente TI.

SIA (Sistemas Informáticos Abiertos), proveedor líder de soluciones de seguridad y servicios de administración de TI, y Everbridge, líder mundial en la gestión de eventos críticos y aplicaciones de software de Continuidad de Negocio, han firmado un acuerdo como socios para ofrecer a las empresas los beneficios de las soluciones unificadas que componen la plataforma de Everbridge

Con esta nueva alianza, SIA incorpora a su actual oferta de seguridad la plataforma de gestión de eventos críticos de Everbridge, que permite garantizar la seguridad de las personas y edificios de una organización para la continuidad del negocio, y la solución IT-Alerting que posibilita evaluar, mitigar y reducir el impacto de cualquier incidente TI, ofreciendo a sus clientes una solución integral para abordar los desafíos de seguridad y, una vez más, de continuidad del negocio.

Para Everbridge este acuerdo supone contar a partir de ahora con elpartner más adecuado en España en términos de Seguridad para proporcionar a sus clientes el valor y el retorno de la inversión de sus soluciones.

Una óptima respuesta a las crisis

Gracias a la tecnología de Everbridge, SIA posibilita con estas aplicaciones **automatizar y acelerar la respuesta a las brechas de seguridad** para la continuidad del negocio proporcionando

el mensaje adecuado a la persona apropiada en el momento oportuno. Por otro lado, **IT Alerting** permitirá a los equipos de soporte de IT comunicarse de manera fluida y eficiente en los momentos de crisis. Esta mejor planificación de respuesta y comunicación ayudará a los clientes a reducir los tiempos de interrupción de sus sistemas más críticos.

Según **Enrique Palomares**, director general de SIA, “las organizaciones de IT cada vez son más complejas de administrar y dar soporte. Esto da lugar además a un aumento del volumen de alertas que se generan. Los clientes necesitan simplificar y optimizar la administración de estas alertas y estamos convencidos de que Everbridge es el mejor socio para dar la respuesta más adecuada".

José Manuel Villanueva, director de Everbridge en España y Portugal, apunta “estamos encantados de ampliar nuestro alcance en España y Portugal a través de esta alianza con SIA para ayudar a las organizaciones a responder mejor al rápido aumento de las necesidades críticas de IT. Su sólida base de clientes y capacidades de servicio profesional impulsarán nuestro crecimiento dentro del mercado".

El acuerdo se enmarca dentro de la política de alianzas estratégicas que SIA viene desarrollando desde hace años a través de la firma de convenios de colaboración con líderes tecnológicos a nivel mundial, reforzando así su apuesta por la especialización, la formación continua y el trabajo en un entorno de colaboración, con el fin de adaptar la TI a las necesidades de sus clientes.

Expansión economía digital 12 Febrero 2019

ANÁLISIS

Spotify no se conforma con la música y quiere liderar los pódcast

La compañía sueca adquiere dos 'start up' con la ambición de construir una alternativa a la radio. **Por M. Prieto**

Spotify busca expandirse más allá de la música en streaming. En un reciente post, Daniel Ek, consejero delegado y cofundador de la compañía sueca, confiesa que el futuro de la compañía es el audio, no sólo la música. "En el futuro, más del 20% del tiempo de escucha en Spotify no será de música", pronostica Ek.

Para ello, Spotify quiere convertirse en la plataforma líder en el ámbito de los pódcast. En ese sentido, la compañía ha adquirido recientemente dos start up, Gimlet y Anchor, por una cifra que, según The Wall Street Journal, supera los 250 millones de dólares. La primera es una compañía centrada en la producción de pódcast narrativos. Por su parte, Anchor ofrece herramientas que permiten crear y distribuir este tipo de contenidos. Además, Spotify ha anunciado que tiene un presupuesto de entre 400 y 500 millones de dólares para seguir adquiriendo compañías.

"Tener contenido más diversificado ayuda a atraer nuevos usuarios, aumentar el nivel de compromiso y reducir la rotación de usuarios. Este movimiento encaja en su plan para alcanzar 1.000 millones de usuarios (frente a 207 millones en la actualidad). Para llegar ahí Spotify tiene que posicionarse como una alternativa real a la radio, para lo que debe ofrecer contenido diverso y también exclusivo", explica Joakim Dal, socio de GP Bullhound, aceleradora de Spotify.

Gimlet produce pódcast narrativos, mientras que Anchor permite su creación y distribución

"En el futuro más del 20% de tiempo de escucha en Spotify no será música", dice Daniel Ek

"La gente dedica más de dos horas diarias a la radio; queremos llevar esa experiencia a Spotify"

Ek está convencido del potencial de negocio de la oferta de contenido de audio. El ejecutivo se muestra convencido por el hecho de que la industria de vídeo tuviese un billón de dólares y la de audio una décima parte. "La gente dedica más de dos horas diarias a escuchar la radio. Nosotros queremos llevar esa experiencia a Spotify", dice Ek. En su opinión, en un momento en el que se vive la proliferación por la cantidad de dispositivos dedicados a los familias, se abre una enorme oportunidad para el audio. Una industria que, según Ek, "crecerá significativamente" al llevarla a Internet.

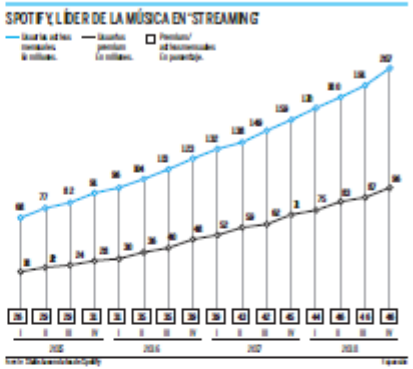
Y el gran paso en esta apuesta es el pódcast, un formato que aporta valor porque, además de atraer a nuevos usuarios, crea mayores vínculos con la plataforma. Según Spotify, los oyentes de pódcast pasan prácticamente el doble de tiempo en Spotify que el resto de usuarios, y dedican también más tiempo a escuchar música.

Además, los pódcast abren a la compañía la oportunidad de convertirse en productor de contenido original, la misma idea que Netflix en el mercado del vídeo. Netflix se decantó por producir contenido para reducir su dependencia de los grandes estudios. Spotify es líder del negocio de la música en streaming, pero eso no que pagar una abultada factura a las discográficas en forma de royalties. "El negocio de pódcast es más rentable a nivel de márgenes, pero es mucho más pequeño que el de la música", apunta Dal.

Gimlet, por ejemplo, es conocida por pódcast narrativos como Reply All, StartUp o Homecoming, lo que, según Ek, coloca a Spotify como el productor líder mundial de pódcast. Así, aporta talento creativo y sitúa a Spotify en el ecosistema de pódcast, dice Dal. "En términos financieros no va a tener mucho impacto en 2019, lo importante es el giro estratégico que la empresa está tomando", añade.

La compañía está convencida de que es el momento de invertir para crecer, a pesar del impacto que pueda tener en sus márgenes. En declaraciones a The Wall Street Journal, Daniel Ek asegura que el hecho de haber alcanzado por primera vez un beneficio operativo en la recta final del año (44 millones de euros) valida su modelo de negocio. En el cuarto trimestre, el segundo con beneficio neto, ganó 442 millones de euros y aumentó un 30% los ingresos hasta 1.600 millones.

SPOTIFY, LÍDER DE LA MÚSICA EN 'STREAMING'



Fuente: Statista basado en datos de Spotify

PISTAS

SIA amplía su cartera de seguridad con la alianza con Everbridge

SIA (Sistemas Informáticos Abiertos), proveedor de soluciones de seguridad y servicios de administración de TI, y Everbridge han firmado un acuerdo para ofrecer a las empresas los beneficios de las soluciones unificadas de la plataforma del grupo americano de gestión de avisos críticos y aplicaciones de software. SIA, compañía de origen español, incorpora así a su oferta de la plataforma de Everbridge, que permite garantizar la seguridad de las personas y edificios de una organización para la continuidad de su negocio.

Fundación Telefónica e Inspiring Girls acercan la Inteligencia Artificial a las más jóvenes

La Fundación Inspiring Girls y la Fundación Telefónica celebraron ayer una jornada en la que 11 mujeres referentes en el ámbito de la ciencia y la tecnología conversaron con 80 niñas para mostrarles cómo en la robótica, en el big data o en la energía pueden encontrar su opción profesional más allá de los estereotipos y etiquetas. La ministra de Industria, Comercio y Turismo, Reyes Maroto, la directora en robótica, Elena García Armada, y la directora general de Twitter en España y Portugal, Nathalie Picquot, fueron algunas de las mujeres que participaron en Las Niñas y la Inteligencia Artificial.

Grupo PSA utiliza tecnología IoT para la trazabilidad

El grupo de automoción PSA ha implantado una solución que permite la trazabilidad de los consumidores entre proveedores y plantas de ensamblaje. Esta solución, basada en las tecnologías Internet de las Cosas (IoT) de IBM y Sigfox, optimiza la rotación de consumidores entre las distintas localizaciones y fábricas de PSA. La solución permite rastrear en tiempo real los consumidores equipados con sensores de Sigfox. IBM, Sigfox y Grupo PSA planean ofrecer esta plataforma a otras fábricas europeas este año.

Yago Castillo, nuevo director general de Antevenio en España

Antevenio ha nombrado a Yago Castillo director general de la compañía en España. Con más de 20 años de experiencia, ha dirigido equipos de ventas en empresas como Telefónica, Microsoft, Vocento o JobaTalent y ha ocupado la dirección general de Terra. En los últimos tres años fue el director comercial de Medios Digitales de Mediaset España. Desde su nueva posición, será el encargado de desarrollar y ejecutar los planes estratégicos de los principales productos de Antevenio y el área de inbound marketing.

computing

18 Marzo 2019

La USC, pionera en utilizar firma cualificada en la nube

Con la solución implementada por SIA, la Universidad de Santiago de Compostela incorpora un sistema de firma electrónica equivalente a la manuscrita bajo el nuevo marco regulatorio eIDAS.

La Universidad de Santiago de Compostela -USC- ha confiado en **SIA (Sistemas Informáticos Abiertos)** para poner en marcha un servicio en la nube (SaaS - Software as a Service) de **firma electrónica cualificada** por parte del usuario final de los documentos generados en los sistemas de información de la universidad que requieren su firma.

Con esta iniciativa, la institución académica dispone de un sistema de firma digital, basado en la emisión y utilización de certificados cualificados centralizados por parte de SIA, que combina la agilidad de su puesta en marcha, la facilidad de uso y todas las garantías de seguridad jurídica que aporta el reglamento UE 910/2014 eIDAS.

Seguridad y usabilidad, de la mano

El proyecto ha sido desplegado inicialmente en el equipo de gobierno de la USC que, a partir de ahora, puede firmar digitalmente cualquier documento desde cualquier dispositivo que posea un navegador y una conexión a Internet, independientemente del lugar desde donde lo haga. Además, esa **firma digital tiene un valor legal equiparable a la firma**

manuscrita.

> La universidad de Santiago de Compostela se convierte en la primera universidad gallega en sacar partido a todas las ventajas de la firma cualificada en la nube

Con la firma digital en la nube de SIA, la universidad afirma conseguir todas las ventajas operativas y legales de la firma digital y eliminar los inconvenientes asociados al despliegue de tarjetas, lectores, drivers, Java, etc.

La universidad de Santiago de Compostela se convierte en la primera universidad gallega en sacar partido a todas las ventajas de la firma cualificada en la nube
Para José Manuel Velo, director del área TIC de la Universidad de Santiago de Compostela, “el éxito del proyecto reside en una excelente combinación de dos factores: por un lado, la calidad del equipo de SIA a nivel de conocimiento, capacidad técnica y rapidez de respuesta; por otro, la altísima competencia del equipo de desarrollo de la USC que ha mostrado una gran eficiencia en su labor de integración con la plataforma de firma de SIA”.

Por su parte, **José Luis Reyes, CTO de SIA**, añade que “el servicio, que se prestará en remoto en **modalidad 24x7x365 y cuya infraestructura de firma se encuentra en la nube de SIA en su totalidad**, dota al personal de la USC de un medio cómodo y seguro de aplicar firmas electrónicas, que mejora la eficiencia de los procesos actuales al tiempo que garantiza la validez legal de las actuaciones realizadas”.

Como resultado, la universidad de Santiago de Compostela se convierte en la primera universidad gallega en sacar partido a todas las ventajas de la firma cualificada en la nube. La iniciativa contempla además la posibilidad de ampliarse al resto de miembros de la comunidad universitaria en un futuro próximo.

SIA amplía su propuesta de soluciones de continuidad con Everbridge

El acuerdo busca contar con una solución integral para evaluar, mitigar y reducir el impacto de cualquier incidente de IT.

SIA (Sistemas Informáticos Abiertos), proveedor de soluciones de seguridad y servicios de administración de TI, y Everbridge, especializada en la gestión de eventos críticos y aplicaciones de software de Continuidad de Negocio, han firmado un acuerdo como socios para ofrecer a las empresas soluciones unificadas que componen la plataforma de Everbridge

Con esta nueva alianza, SIA incorpora a su actual oferta de seguridad la plataforma de gestión de eventos críticos de Everbridge, que permite garantizar la seguridad de las personas y edificios de una organización para la continuidad del negocio, y la solución IT-Alerting que posibilita evaluar, mitigar y reducir el impacto de cualquier incidente TI.

Para Everbridge este acuerdo supone contar a partir de ahora con el partner más adecuado en España en términos de seguridad para proporcionar a sus clientes el valor y el retorno de la inversión de sus soluciones.

Una óptima respuesta a las crisis

Gracias a la tecnología de Everbridge, SIA posibilita con estas aplicaciones automatizar y acelerar la respuesta a las brechas

de seguridad para la continuidad del negocio proporcionando el mensaje adecuado a la persona apropiada en el momento oportuno. Por otro lado, IT Alerting permitirá a los equipos de soporte de IT comunicarse de manera fluida y eficiente en los momentos de crisis.

SIA posibilita con estas aplicaciones automatizar y acelerar la respuesta a las brechas de seguridad para la continuidad del negocio

Según **Enrique Palomares, director general de SIA**, “las organizaciones de IT cada vez son más complejas de administrar y dar soporte. Esto da lugar además a un aumento del volumen de alertas que se generan. Los clientes necesitan simplificar y optimizar la administración de estas alertas y estamos convencidos de que Everbridge es el mejor socio para dar la respuesta más adecuada".

José Manuel Villanueva, director de Everbridge en España y Portugal, apunta “estamos encantados de ampliar nuestro alcance en España y Portugal a través de esta alianza con SIA para ayudar a las organizaciones a responder mejor al rápido aumento de las necesidades críticas de IT. Su sólida base de clientes y capacidades de servicio profesional impulsarán nuestro crecimiento dentro del mercado".

El acuerdo se enmarca en la política de alianzas estratégicas que SIA viene desarrollando desde hace años a través de la firma de convenios de colaboración con líderes tecnológicos a nivel mundial, reforzando así su apuesta por la especialización, la formación continua y el trabajo en un entorno de colaboración.

elEconomista.es

15 Marzo 2019

La USC elige a SIA para convertirse en la primera universidad gallega en utilizar firma cualificada en la nube

La Universidad de Santiago de Compostela -USC- ha confiado en SIA (Sistemas Informáticos Abiertos), proveedor líder de soluciones de seguridad y servicios de administración de TI, para poner en marcha un servicio en la nube (SaaS - Software as a Service) de firma electrónica cualificada por parte del usuario final de los documentos generados en los sistemas de información de la universidad que requieren su firma.

Con esta iniciativa, la institución académica dispone de un sistema de firma digital, basado en la emisión y utilización de certificados cualificados centralizados por parte de SIA, que combina la agilidad de su puesta en marcha, la facilidad de uso y todas las garantías de seguridad jurídica que aporta el reglamento UE 910/2014 eIDAS.

Seguridad y usabilidad, de la mano

El proyecto ha sido desplegado inicialmente en el equipo de gobierno de la USC que, a partir de ahora, puede firmar digitalmente cualquier documento desde cualquier dispositivo que posea un navegador y una conexión a internet, independientemente del lugar desde donde lo haga. Además, esa firma digital tiene un valor legal equiparable a la firma manuscrita.

Con la firma digital en la nube de SIA, la universidad consigue todas las ventajas operativas y legales de la firma digital y se eliminan los inconvenientes asociados al despliegue de tarjetas, lectores, drivers, Java, etc. En definitiva, dota al usuario de un

medio cómodo, seguro y con el mínimo coste operativo.

Para José Manuel Velo, director del área TIC de la Universidad de Santiago de Compostela, "el éxito del proyecto reside en una excelente combinación de dos factores: por un lado, la calidad del equipo de SIA a nivel de conocimiento, capacidad técnica y rapidez de respuesta; por otro, la altísima competencia del equipo de desarrollo de la USC que ha mostrado una gran eficiencia en su labor de integración con la plataforma de firma de SIA".

Por su parte, José Luis Reyes, CTO de SIA, añade que "el servicio, que se prestará en remoto en modalidad 24x7x365 y cuya infraestructura de firma se encuentra en la nube de SIA en su totalidad, dota al personal de la USC de un medio cómodo y seguro de aplicar firmas electrónicas, que mejora la eficiencia de los procesos actuales al tiempo que garantiza la validez legal de las actuaciones realizadas".

Como resultado, la universidad de Santiago de Compostela se convierte en la primera universidad gallega en sacar partido a todas las ventajas de la firma cualificada en la nube. La iniciativa contempla además la posibilidad de ampliarse al resto de miembros de la comunidad universitaria en un futuro próximo

La Universidad de Santiago de Compostela implanta firma cualificada en la nube

La universidad avanza en su estrategia de transformación digital, incorporando en sus aplicaciones un sistema de firma electrónica del Grupo SIA equivalente a la manuscrita bajo el nuevo marco regulatorio Eidas.

La Universidad de Santiago de Compostela ha confiado en SIA (Sistemas Informáticos Abiertos), proveedor de soluciones de seguridad y servicios de administración de TI, para poner en marcha un servicio en la nube (SaaS - Software as a Service) de firma electrónica cualificada por parte del usuario final de los documentos generados en los sistemas de información de la universidad que requieren su firma.

Con esta iniciativa, la institución académica dispone de un sistema de firma digital, basado en la emisión y utilización de certificados cualificados centralizados por parte de SIA, que combina la agilidad de su puesta en marcha, la facilidad de uso y todas las garantías de seguridad jurídica que aporta el reglamento UE 910/2014 eIDAS.

El proyecto ha sido desplegado inicialmente en el equipo de gobierno de la USC que, a partir de ahora, puede firmar digitalmente cualquier documento desde cualquier dispositivo que posea un navegador y una conexión a internet, independientemente del lugar desde donde lo haga. Además, esa firma digital tiene un valor legal equiparable a la firma manuscrita.

Con la firma digital en la nube de SIA, la universidad consigue todas las ventajas operativas y legales de la firma digital y se eliminan los inconvenientes asociados al despliegue de tarjetas,

, lectores, drivers, Java, etc. En definitiva, dota al usuario de un medio cómodo, seguro y con el mínimo coste operativo.

Para José Manuel Velo, director del área TIC de la Universidad de Santiago de Compostela, “el éxito del proyecto reside en una excelente combinación de dos factores: por un lado, la calidad del equipo de SIA a nivel de conocimiento, capacidad técnica y rapidez de respuesta; por otro, la altísima competencia del equipo de desarrollo de la USC que ha mostrado una gran eficiencia en su labor de integración con la plataforma de firma de SIA”.

Por su parte, José Luis Reyes, CTO de SIA, añade que “el servicio, que se prestará en remoto en modalidad 24x7x365 y cuya infraestructura de firma se encuentra en la nube de SIA en su totalidad, dota al personal de la USC de un medio cómodo y seguro de aplicar firmas electrónicas, que mejora la eficiencia de los procesos actuales al tiempo que garantiza la validez legal de las actuaciones realizadas”.

Como resultado, la universidad de Santiago de Compostela se convierte en la primera universidad gallega en sacar partido a todas las ventajas de la firma cualificada en la nube. La iniciativa contempla además la posibilidad de ampliarse al resto de miembros de la comunidad universitaria en un futuro próximo.

La Universidad de Santiago elige a SIA para utilizar firma cualificada en la nube

La Universidad de Santiago de Compostela -USC- ha confiado en SIA (Sistemas Informáticos Abiertos) para poner en marcha un servicio en la de firma electrónica cualificada por parte del usuario final de los documentos generados en los sistemas de información de la universidad que requieren su firma.

Con esta iniciativa, la institución académica dispone de un sistema de firma digital, basado en la emisión y utilización de certificados cualificados centralizados por parte de SIA, que combina la agilidad de su puesta en marcha, la facilidad de uso y todas las garantías de seguridad jurídica que aporta el reglamento UE 910/2014 eIDAS.

Seguridad y usabilidad, de la mano

El proyecto ha sido desplegado inicialmente en el equipo de gobierno de la Universidad de Santiago que, a partir de ahora, puede firmar digitalmente cualquier documento desde cualquier dispositivo que posea un navegador y una conexión a internet, independientemente del lugar desde donde lo haga. Además, esa firma digital tiene un valor legal equiparable a la firma manuscrita.

El proyecto ha sido desplegado inicialmente en el equipo de gobierno de la Universidad de Santiago que, a partir de ahora, puede firmar digitalmente cualquier documento desde cualquier dispositivo

Con la firma digital en la nube de SIA, la universidad consigue todas las ventajas operativas y legales de la firma digital y se eliminan los inconvenientes asociados al despliegue de tarjetas, lectores, drivers, Java, etc. En definitiva, dota al usuario de un medio cómodo, seguro y con el mínimo coste operativo.

Para José Manuel Velo, director del área TIC de la Universidad de Santiago de Compostela, “el éxito del proyecto reside en una excelente combinación de dos factores: por un lado, la calidad del equipo de SIA a nivel de conocimiento, capacidad técnica y rapidez de respuesta; por otro, la altísima competencia del equipo de desarrollo de la USC que ha mostrado una gran eficiencia en su labor de integración con la plataforma de firma de SIA”.

Por su parte, José Luis Reyes, CTO de SIA, añade que “el servicio, que se prestará en remoto en modalidad 24x7x365 y cuya infraestructura de firma se encuentra en la nube de SIA en su totalidad, dota al personal de la USC de un medio cómodo y seguro de aplicar firmas electrónicas, que mejora la eficiencia de los procesos actuales al tiempo que garantiza la validez legal de las actuaciones realizadas”.

Como resultado, la universidad de Santiago de Compostela se convierte en la primera universidad gallega en sacar partido a todas las ventajas de la firma cualificada en la nube. La iniciativa contempla además la posibilidad de ampliarse al resto de miembros de la comunidad universitaria en un futuro próximo.

La Universidade de Santiago de Compostela implanta un sistema de firma digita

La firma SIA ha colaborado con la institución académica en el despliegue del servicio SaaS de rúbrica electrónica, acorde con la última normativa europea sobre el tema.

La Universidade de Santiago de Compostela, la USC, se actualiza para facilitar la gestión a los usuarios de sus sistemas de información. La institución ha puesto en marcha un proyecto para integrar la firma digital y se convierte así en el primer centro de su tipo en Galicia en incorporar esta modalidad de servicio cualificado en la nube.

El organismo ha contado con la colaboración de la firma SIA, especializada en soluciones de seguridad y servicios de administración de TI, en el desarrollo del proyecto de SaaS de firma digital. Este permite la emisión y utilización de certificados cualificados centralizados, de acuerdo a la normativa UE 910/2014 eIDAS, que establece el marco legal en Europa para la identificación electrónica.

Con esta iniciativa, los usuarios pueden firmar de forma digital cualquier documento, para lo cual solo necesitan un dispositivo que posea un navegador y una conexión a internet. La rúbrica electrónica tiene un valor legal equiparable al de la manuscrita, con lo que se gana en agilidad, simplicidad operativa y ahorro económico al no necesitarse logística añadida, como tarjetas, lectores o la instalación de programas o drivers específicos.

El proyecto ha sido desplegado inicialmente en el equipo de gobierno de la USC, aunque podría ampliarse al resto de miembros de la comunidad universitaria.

Desde SIA, su CTO, José Luis Reyes, destaca que “el servicio, que se prestará en remoto en modalidad 24x7x365 y cuya infraestructura de firma se encuentra en la nube de SIA en su totalidad” permite mejorar “la eficiencia de los procesos actuales al tiempo que garantiza la validez legal de las actuaciones realizadas”.

Para el director del área TIC de la USC, José Manuel Velo, el éxito de la iniciativa está, básicamente, en los equipos, tanto en “la calidad del equipo de SIA a nivel de conocimiento, capacidad técnica y rapidez de respuesta” como en “la altísima competencia del equipo de desarrollo de la USC, que ha mostrado una gran eficiencia en su labor de integración con la plataforma de firma de SIA”.

redseguridad.com

18 Marzo 2019

La USC apuesta por SIA para implantar la firma cualificada en la nube

Se trata de la primera universidad gallega en poner en marcha este servicio que equivale a la firma manuscrita.

La Universidad de Santiago de Compostela (USC) ha confiado en SIA (Sistemas Informáticos Abiertos) para implantar un servicio en la nube de firma electrónica cualificada por parte del usuario final de los documentos generados en los sistemas de información de la universidad que requieren su firma. Con esta iniciativa, pionera entre las universidades gallegas, esta institución académica dispone de un sistema de firma digital, basado en la emisión y utilización de certificados cualificados centralizados por parte de SIA, que combina la agilidad de su puesta en marcha, la facilidad de uso y todas las garantías de seguridad jurídica que aporta el reglamento UE 910/2014 eIDAS.

El proyecto ha sido desplegado inicialmente en el equipo de gobierno de la USC que, a partir de ahora, puede firmar digitalmente cualquier documento desde cualquier dispositivo que posea un navegador y una conexión a Internet, independientemente del lugar desde donde lo haga. Además, esa firma digital tiene un valor legal equiparable a la firma manuscrita. Con este paso, la universidad consigue todas las ventajas operativas y legales de la firma digital y se eliminan los inconvenientes asociados al despliegue de tarjetas, lectores, drivers, Java, etc.

Para José Manuel Velo, director del área TIC de la Universidad de Santiago de Compostela, “el éxito del proyecto reside en una excelente combinación de dos factores: por un lado, la calidad del equipo de SIA en cuanto a conocimiento, capacidad técnica y rapidez de respuesta; por otro, la altísima competencia del equipo de desarrollo de la USC, que ha mostrado una gran eficiencia en su labor de integración con la plataforma de firma de SIA”.

Por su parte, José Luis Reyes, CTO de SIA, añade: “El servicio, que se prestará en remoto en modalidad 24x7x365 y cuya infraestructura de firma se encuentra en la nube de SIA en su totalidad, dota al personal de la USC de un medio cómodo y seguro de aplicar firmas electrónicas, que mejora la eficiencia de los procesos actuales, al tiempo que garantiza la validez legal de las actuaciones realizadas”, concluye.

La USC elige a SIA para convertirse en la primera universidad gallega en utilizar firma cualificada en la nube

La Universidad de Santiago de Compostela ha confiado en SIA para poner en marcha un servicio en la nube de firma electrónica cualificada por parte del usuario final de los documentos generados en los sistemas de información de la universidad que requieren su firma

Con esta iniciativa, la Universidad de Santiago de Compostela (USC) dispone de un sistema de firma digital, basado en la emisión y utilización de certificados cualificados centralizados por parte de SIA (Sistemas Informáticos Abiertos), que combina la agilidad de su puesta en marcha, la facilidad de uso y todas las garantías de seguridad jurídica que aporta el reglamento UE 910/2014 eIDAS.

El proyecto ha sido desplegado inicialmente en el equipo de gobierno de la USC que, a partir de ahora, puede firmar digitalmente cualquier documento desde cualquier dispositivo que posea un navegador y una conexión a internet, independientemente del lugar desde donde lo haga. Además, esa firma digital tiene un valor legal equiparable a la firma manuscrita.

Con la firma digital en la nube de SIA, la universidad consigue todas las ventajas operativas y legales de la firma digital y se eliminan los inconvenientes asociados al despliegue de tarjetas, lectores, drivers, Java, etc. En definitiva, dota al usuario de un medio cómodo, seguro y con el mínimo coste operativo.

Seguridad, usabilidad y mejora de la eficiencia

Para José Manuel Velo, director del área TIC de la Universidad de Santiago de Compostela, “el éxito del proyecto reside en una excelente combinación de dos factores: por un lado, la

calidad del equipo de SIA a nivel de conocimiento, capacidad técnica y rapidez de respuesta; por otro, la altísima competencia del equipo de desarrollo de la USC que ha mostrado una gran eficiencia en su labor de integración con la plataforma de firma de SIA".

Por su parte, José Luis Reyes, CTO de SIA, añade que "el servicio, que se prestará en remoto en modalidad 24x7x365 y cuya infraestructura de firma se encuentra en la nube de SIA en su totalidad, dota al personal de la USC de un medio cómodo y seguro de aplicar firmas electrónicas, que mejora la eficiencia de los procesos actuales al tiempo que garantiza la validez legal de las actuaciones realizadas".

Como resultado, la universidad de Santiago de Compostela se convierte en la primera universidad gallega en sacar partido a todas las ventajas de la firma cualificada en la nube. La iniciativa contempla además la posibilidad de ampliarse al resto de miembros de la comunidad universitaria en un futuro próximo.

	Empresa	Fact. 18*	Fact. 17*	Incremento	Plantilla 18	Plantilla 17	Incremento	País
51	Sermicro	125,3	128,0	-2,1	2.550	2.450	2,3	España
52	GyD	122,6	68,6	78,7	711	604	17,7	Alemania
53	DMI	115,0	112,0	2,7	110	105	4,8	España
54	Grupo VASS	110,0	84,5	30,3	1629	1312	24,2	España
55	Unisono	107,0	106,1	0,8	5.000	4.960	0,8	España
56	Diebold Nixdorf	94,9	92,8	2,3	204	206	-1,0	Alemania
57	NCR	90,0	88,0	2,3	215	220	-2,3	EEUU
58	Atos	89,9	80,0	12,4	2.000	1.800	11,1	Francia
59	VOZ.COM	89,0	68,0	30,9	60	48	25,0	España
60	Valoriza	86,0	81,0	6,2	120	118	1,7	Polonia
61	Epson	85,4	84,3	1,3	126	120	5,0	Japón
62	Cisco Systems	85,0	87,0	-2,3	312	339	-8,0	EEUU
63	Infortisa	83,0	83,0	0,0	120	98	22,4	España
64	Telecoming	81,0	68,0	19,1	131	116	12,9	España
65	Aspe Consulting	79,0	72,0	9,7	1.600	1.590	0,6	España
66	Kyocera Document Solutions	78,0	67,0	16,4	148	148	-2,0	Japón
67	Konica Minolta	73,8	70,3	5,0	341	321	6,2	Japón
68	Xerox	73,0	71,0	2,8	450	440	2,3	Reino Unido
69	Altia	69,3	64,7	7,0	902	783	10,9	España
70	Sidec	63,7	68,2	-6,6	405	404	0,2	España
71	Celestica Valencia	63,3	47,3	34,0	391	266	43,2	Canadá
72	Software AG	61,0	70,4	-13,3	554	601	-7,8	Alemania
73	Exclusive Networks	60,0	57,0	5,3	48	45	6,7	Francia
74	Neoris	60,0	58,0	3,4	800	782	2,3	Holanda
75	Micro Focus	59,0	60,0	-1,7	190	210	-9,5	Reino Unido
76	Entelgy	58,5	58,4	0,2	1.170	1.170	0,0	España
77	IPM	58,5	48,2	21,3	130	135	-3,7	España
78	Toshiba TEC	58,0	56,0	5,5	76	69	10,1	Japón
79	Eleaingo	58,0	52,5	10,5	900	850	5,9	España
80	aSistemas	58,0	45,5	27,5	1.209	954	26,7	España
81	Computerf	56,0	53,0	5,7	600	620	-7,7	España
82	Compana	55,0	56,0	-1,8	140	145	-3,4	Alemania
83	Brighstar2020 Mobile	54,4	66,8	-18,6	51	76	-32,9	EEUU
84	Arsys	53,0	47,0	12,8	318	311	2,3	España
85	Hitachi Vantara	53,0	52,0	1,9	78	80	-2,5	EEUU
86	Acens	52,7	48,0	9,8	243	244	-0,4	España
87	Infowork	52,0	44,0	18,2	65	65	0,0	España
88	Ciberoc	51,0	49,0	4,1	650	640	1,2	España
89	Bechtle	51,0	47,0	8,5	71	70	1,4	Alemania
90	Satlink	50,3	48,0	4,8	50	48	4,2	España
91	Equinix	50,0	51,0	-2,0	260	304	-14,5	EEUU
92	Sistemas Informáticos Abiertos	47,6	41,0	16,5	646	557	16,0	España
93	Technidge	46,0	43,0	7,0	435	423	2,8	España
94	Abast	45,3	41,0	10,5	390	350	8,6	España
95	Almira	45,0	40,0	12,5	826	740	11,6	España
96	Salicru	45,0	41,5	8,4	218	191	14,1	España
97	Grupo CMC	44,4	29,5	50,4	791	624	26,8	España
98	Inycom	40,3	73,0	-44,8	750	720	4,2	España
99	Inerbis	39,5	25,6	54,1	476	336	41,7	España
100	Sogeti	39,4	28,7	37,6	700	627	11,6	Francia

*Cifras en millones de euros / Estimaciones Computing / Elaboración propia

	Empresa	Fact. 18*	Fact. 17*	Incremento	Plantilla 18	Plantilla 17	Incremento	País
101	Solfium	39,2	28,7	36,6	152	100	52,0	España
102	Metal4	37,0	33,0	12,1	563	530	6,2	España
103	Softland Inversiones	33,6	29,8	12,8	737	543	35,7	España
104	Omega Peripherals	33,0	38,0	-13,2	130	115	13,0	España
105	SAS Institute	32,5	31,7	2,5	120	119	0,8	EEUU
106	Infinion	32,0	30,0	6,7	30	26	15,4	Holanda
107	CGI Group	32,0	33,0	-3,0	550	580	-5,2	Canadá
108	Unitronics Comunicaciones	31,5	30,2	4,3	260	260	0,0	España
109	Sensaco	31,1	26,6	16,7	697	629	9,2	España
110	Davoltram Drago	30,0	25,0	20,0	583	580	0,5	Francia
111	SPC	29,1	29,4	-1,1	50	52	-3,8	España
112	Unit4	29,0	28,5	1,8	270	265	1,9	Holanda
113	Sabel	28,5	24,0	18,8	524	495	5,9	España
114	Prodemans	27,0	25,7	5,1	300	270	11,1	Francia
115	Arpan Comunicaciones	26,8	24,7	8,2	62	61	1,6	España
116	Ilunion IT Services	26,5	24,9	6,4	166	110	50,9	España
117	Ingecom	25,0	23,0	8,7	24	24	0,0	España
118	Grobaico	24,7	23,0	7,4	172	170	1,2	España
119	Landalsi	24,0	24,8	-3,2	35	35	0,0	España
120	Primavera BSS	23,4	22,3	4,9	300	280	7,1	Portugal
121	Alhambra-Eidos	22,2	20,4	8,8	189	183	3,3	Francia
122	Panel Sistemas Informáticos	20,5	19,1	7,3	400	392	2,0	España
123	BMC Software	18,8	17,6	6,8	88	83	6,0	EEUU
124	Global Switch	18,5	17,6	5,1	12	13	-7,7	Reino Unido
125	EraseNet	18,5	17,0	8,8	150	135	20,0	España
126	Fibratel	17,4	14,3	21,5	120	105	14,3	España
127	Consenaln	17,0	19,1	-11,0	407	316	28,8	España
128	Aradal Consulting	16,8	15,5	8,4	170	140	21,4	España
129	Sarenet	16,0	16,7	-4,2	80	80	0,0	España
130	Consas	16,0	14,6	9,6	300	292	2,7	España
131	S2 Grupo	15,5	10,5	47,6	288	232	24,1	España
132	ADEA	14,5	13,9	4,0	157	178	-11,8	España
133	Zucchetti	14,0			200			España
134	Ozona	13,5	13,0	3,8	63	63	0,0	España
135	Commsult	13,4	11,5	16,5	17	17	0,0	EEUU
136	Prosol	12,5	10,9	14,7	58	50	16,0	España
137	Ambance	12,0	10,6	13,2	300	285	5,3	España
138	Serso	11,5	11,2	2,7	93	84	9,5	Francia
139	PHC Software	11,5	10,8	6,5	180	180	0,0	Portugal
140	VozTelecom	11,0	9,8	12,2	155	150	3,3	España
141	Gesein	10,8	9,9	9,2	244	219	11,4	España
142	Altim	10,7	9,4	13,8	100	83	20,5	España
143	Grupo Castilla	10,7	9,3	15,1	164	152	7,9	España
144	Gigaset	10,2	9,6	6,5	12	12	0,0	alemania
145	Avanzo	9,5	8,3	15,0	170	150	13,3	España
146	Fihoca	9,3	9,9	-6,7	135	124	8,9	España
147	Flytech	9,2	8,9	2,9	22	22	0,0	España
148	IMCS Group	8,4	8,6	-3,0	108	115	-6,1	España
149	Information Builders	8,0	7,9	1,3	95	95	0,0	EEUU
150	Pholoria	8,0	6,9	15,9	162	150	10,0	España

*Cifras en millones de euros / Estimaciones Computing / Elaboración propia

computing

27 Marzo 2019

Mutua Universal adopta el servicio de firma en la nube de SIA

La entidad obtiene una notable mejora en la eficiencia y ahorro de costes en los procesos internos, al tiempo que se garantiza la plena validez legal de la documentación contractual firmada

Mutua Universal MUGENAT ha elegido a SIA (Sistemas Informáticos Abiertos) para poner en marcha un sistema de firma digital en la nube con objeto de evolucionar hacia una oficina digital y abordar sus procesos de una manera ágil y con plenas garantías legales mediante firma electrónica cualificada bajo el reglamento eIDAS, equivalente a la firma manuscrita.

La propuesta de SIA cubre tanto los servicios de emisión y gestión de los certificados cualificados como el uso de estos para la firma centralizada, de manera integrada con sus aplicaciones de negocio y, por tanto, en completa movilidad -sin necesidad de ningún componente cliente instalado en el dispositivo del usuario-, o desde las aplicaciones de escritorio, mediante un agente software instalado en los puestos de trabajo para la autenticación y firma ante organismos oficiales.

Hacia una oficina sin papel

Hace más de un año se implantó un sistema de firma biométrica y ya se han firmado en esta modalidad casi dos millones de documentos y se dispone de 28 formularios integrados con la solución, mejorando los tiempos de atención

al paciente. “Con el impulso en el uso de certificados digitales eliminaremos el papel de nuestros procesos que requieren firma, sustituyendo la firma manuscrita mediante firma electrónica, con el fin de evolucionar hacia una oficina sin papel”, destaca Esther Felix, directora de Digitalización de Mutua Universal.

La entidad comenzó un proyecto para dotar a los empleados de un certificado digital para 400 usuarios; quiso potenciar su uso y extenderlo hasta 2.500 usuarios y a un mayor número de procesos en los que se utilizan. Todo ello, mediante una plataforma cloud que aportase seguridad y confianza en entornos productivos de máxima exigencia, para lo cual SIA resultó adjudicataria del proyecto a través de licitación pública.

> Con el impulso en el uso de certificados digitales eliminaremos el papel de nuestros procesos que requieren firma

Además de la cobertura legal que ofrece SIA y la eliminación de las barreras tecnológicas que aporta la solución -firma en la nube sin necesidad de drivers ni instalación de agentes en sistemas finales-, los empleados de Mutua Universal “disponen a partir de ahora de todas las ventajas operativas y legales de la firma digital”, según Marc Muntañá, director técnico de Control y Reporting de Mutua Universal.

Con el despliegue de la iniciativa, la entidad afirma lograr ahorrar tiempo y costes en sus procesos internos y contar con las garantías de seguridad jurídica que aporta el reglamento UE 910/2014 eIDAS mediante una plataforma tecnológica fácil de usar y respetuosa con el medio ambiente. Además, la solución proporcionará a los usuarios finales comodidad al evitar los desplazamientos, accesibilidad al firmar en cualquier momento y desde cualquier lugar y sencillez al realizar la firma desde cualquier dispositivo con acceso a internet.

Con esta y otras iniciativas, Mutua Universal sigue avanzando en su proceso de Innovación y Transformación Digital para responder a las necesidades actuales de sus asociados. La estrategia digital de la entidad sitúa a los mutualistas en el centro del proceso, con el objetivo de desarrollar soluciones con un beneficio práctico e inmediato para ellos.

Tecnología de confianza y conocimiento experto

El éxito del proyecto ha residido en tres pilares fundamentales: la **cualificación eIDAS de los servicios que presta SIA a través de SIACERT TrustedServices**; los máximos niveles de seguridad y certificación de la tecnología de SIAVAL SafeCert, utilizada para la firma en la nube y certificada como dispositivo cualificado de creación de firma (QSCD) a nivel europeo; y, como apunta Muntañá, "*la combinación de la experiencia, alto conocimiento y desempeño de sus profesionales en el desarrollo de proyectos similares en el ámbito de la Firma Electrónica, tanto desde un punto de vista técnico como legal, y de la facilidad de implantación de la solución por parte del equipo de Digitalización y Tecnología de Mutua Universal*".

Por su parte, Alfonso Fernández, director de Desarrollo de Negocio en SIA, señala que "***estamos totalmente satisfechos con haber podido proporcionar la mejor respuesta a las necesidades de Mutua Universal***, *aportando toda nuestra experiencia tanto en firma electrónica como en su aplicación dentro del ámbito sanitario donde se requiere máxima disponibilidad y facilidad de uso, y acompañarla en el avance de su proceso de Transformación Digital, mejorando la gestión de sus procesos internos y agilizando los trámites administrativos con los mutualistas y asociados*".

Mutua Universal impulsa su transformación digital con el servicio de firma en la nube de SIA

Gracias a esta iniciativa, Mutua Universal obtiene una notable mejora en la eficiencia y ahorro de costes en los procesos internos, al tiempo que se garantiza la plena validez legal de la documentación contractual firmada.

Mutua Universal MUGENAT, Mutua Colaboradora con la Seguridad Social número 10, ha elegido a SIA (Sistemas Informáticos Abiertos), proveedor líder de soluciones de seguridad y servicios de administración de TI, para poner en marcha un sistema de firma digital en la nube que permite a la entidad evolucionar hacia una oficina digital y abordar sus procesos de una manera ágil y con plenas garantías legales mediante firma electrónica cualificada bajo el reglamento eIDAS, equivalente a la firma manuscrita.

La propuesta de SIA cubre tanto los servicios de emisión y gestión de los certificados cualificados como el uso de los mismos para la firma centralizada, de manera integrada con sus aplicaciones de negocio y, por tanto, en completa movilidad -sin necesidad de ningún componente cliente instalado en el dispositivo del usuario-, o desde las aplicaciones de escritorio, mediante un agente software instalado en los puestos de trabajo para la autenticación y firma ante organismos oficiales.

Hacia una oficina sin papel

Hace más de un año se implantó un sistema de firma biométrica y ya se han firmado en esta modalidad casi dos millones de documentos y se dispone de 28 formularios integrados con la solución, mejorando los tiempos de atención al paciente. “Con el impulso en el uso de certificados digitales eliminaremos el papel de nuestros procesos que requieren

papel", destaca Esther Felix, directora de Digitalización de Mutua Universal.

La entidad comenzó un proyecto para dotar a los empleados de un certificado digital para 400 usuarios; quiso potenciar su uso y extenderlo hasta 2.500 usuarios y a un mayor número de procesos en los que se utilizan. Todo ello, mediante una plataforma cloud que aportase seguridad y confianza en entornos productivos de máxima exigencia, para lo cual SIA resultó adjudicataria del proyecto a través de licitación pública.

Además de la cobertura legal que ofrece SIA y la eliminación de las barreras tecnológicas que aporta la solución -firma en la nube sin necesidad de drivers ni instalación de agentes en sistemas finales-, los empleados de Mutua Universal "disponen a partir de ahora de todas las ventajas operativas y legales de la firma digital", según Marc Muntañá, director técnico de Control y Reporting de Mutua Universal.

Con el despliegue de la iniciativa, la entidad logra ahorrar tiempo y costes en sus procesos internos y contar con las garantías de seguridad jurídica que aporta el reglamento UE 910/2014 eIDAS mediante una plataforma tecnológica fácil de usar y respetuosa con el medio ambiente. Además, la solución proporcionará a los usuarios finales comodidad al evitar los desplazamientos, accesibilidad al firmar en cualquier momento y desde cualquier lugar y sencillez al realizar la firma desde cualquier dispositivo con acceso a internet.

Con esta y otras iniciativas, Mutua Universal sigue avanzando en su proceso de Innovación y Transformación Digital para responder a las necesidades actuales de sus asociados. La estrategia digital de la entidad sitúa a los mutualistas en el centro del proceso, con el objetivo de desarrollar soluciones con un beneficio práctico e inmediato para ellos.

Tecnología de confianza y conocimiento experto

El éxito del proyecto ha residido en tres pilares fundamentales: la cualificación eIDAS de los servicios que presta SIA a través de SIACERT TrustedServices; los máximos niveles de seguridad y certificación de la tecnología de SIAVAL SafeCert, utilizada para la firma en la nube y certificada como dispositivo cualificado de

creación de firma (QSCD) a nivel europeo; y, como apunta Muntañá, “la combinación de la experiencia, alto conocimiento y desempeño de sus profesionales en el desarrollo de proyectos similares en el ámbito de la Firma Electrónica, tanto desde un punto de vista técnico como legal, y de la facilidad de implantación de la solución por parte del equipo de Digitalización y Tecnología de Mutua Universal”.

Por su parte, Alfonso Fernández, director de Desarrollo de Negocio en SIA, señala que “estamos totalmente satisfechos con haber podido proporcionar la mejor respuesta a las necesidades de Mutua Universal, aportando toda nuestra experiencia tanto en firma electrónica como en su aplicación dentro del ámbito sanitario donde se requiere máxima disponibilidad y facilidad de uso, y acompañarla en el avance de su proceso de Transformación Digital, mejorando la gestión de sus procesos internos y agilizando los trámites administrativos con los mutualistas y asociados”.

Gracias a esta iniciativa, la entidad obtiene una notable mejora en la eficiencia y ahorro de costes en los procesos internos

Mutua Universal impulsa su transformación digital con el servicio de firma en la nube de SIA

Mutua Universal MUGENAT, Mutua Colaboradora con la Seguridad Social número 10, ha elegido a SIA (Sistemas Informáticos Abiertos), proveedor de soluciones de seguridad y servicios de administración de TI, para poner en marcha un sistema de firma digital en la nube que permite a la entidad evolucionar hacia una oficina digital y abordar sus procesos de una manera ágil y con plenas garantías legales mediante firma electrónica cualificada bajo el reglamento eIDAS, equivalente a la firma manuscrita.

La propuesta de SIA cubre tanto los servicios de emisión y gestión de los certificados cualificados como el uso de los mismos para la firma centralizada, de manera integrada con sus aplicaciones de negocio y, por tanto, en completa movilidad -sin necesidad de ningún componente cliente instalado en el dispositivo del usuario-, o desde las aplicaciones de escritorio, mediante un agente software instalado en los puestos de trabajo para la autenticación y firma ante organismos oficiales.

Hacia una oficina sin papel

Hace más de un año se implantó un sistema de firma biométrica y ya se han firmado en esta modalidad casi dos millones de documentos y se dispone de 28 formularios integrados con la solución, mejorando los tiempos de atención al paciente. “Con el impulso en el uso de certificados digitales eliminaremos el papel de nuestros procesos que requieren firma, sustituyendo la firma manuscrita mediante firma electrónica, con el fin de

evolucionar hacia una oficina sin papel", destaca Esther Felix, directora de Digitalización de Mutua Universal.

La entidad comenzó un proyecto para dotar a los empleados de un certificado digital para 400 usuarios; quiso potenciar su uso y extenderlo hasta 2.500 usuarios y a un mayor número de procesos en los que se utilizan. Todo ello, mediante una plataforma cloud que aportase seguridad y confianza en entornos productivos de máxima exigencia, para lo cual SIA resultó adjudicataria del proyecto a través de licitación pública.

Además de la cobertura legal que ofrece SIA y la eliminación de las barreras tecnológicas que aporta la solución -firma en la nube sin necesidad de drivers ni instalación de agentes en sistemas finales-, los empleados de Mutua Universal "disponen a partir de ahora de todas las ventajas operativas y legales de la firma digital", según Marc Muntañá, director técnico de Control y Reporting de Mutua Universal.

Con el despliegue de la iniciativa, la entidad logra ahorrar tiempo y costes en sus procesos internos y contar con las garantías de seguridad jurídica que aporta el reglamento UE 910/2014 eIDAS mediante una plataforma tecnológica fácil de usar y respetuosa con el medio ambiente. Además, la solución proporcionará a los usuarios finales comodidad al evitar los desplazamientos, accesibilidad al firmar en cualquier momento y desde cualquier lugar y sencillez al realizar la firma desde cualquier dispositivo con acceso a internet.

Con esta y otras iniciativas, Mutua Universal sigue avanzando en su proceso de Innovación y Transformación Digital para responder a las necesidades actuales de sus asociados. La estrategia digital de la entidad sitúa a los mutualistas en el centro del proceso, con el objetivo de desarrollar soluciones con un beneficio práctico e inmediato para ellos.

Tecnología de confianza y conocimiento experto

El éxito del proyecto ha residido en tres pilares fundamentales: la cualificación eIDAS de los servicios que presta SIA a través de SIACERT TrustedServices; los máximos niveles de seguridad y certificación de la tecnología de SIAVAL SafeCert, utilizada para la firma en la nube y certificada como dispositivo cualificado de

creación de firma (QSCD) a nivel europeo; y, como apunta Muntañá, “la combinación de la experiencia, alto conocimiento y desempeño de sus profesionales en el desarrollo de proyectos similares en el ámbito de la Firma Electrónica, tanto desde un punto de vista técnico como legal, y de la facilidad de implantación de la solución por parte del equipo de Digitalización y Tecnología de Mutua Universal”.

Por su parte, Alfonso Fernández, director de Desarrollo de Negocio en SIA, señala que “estamos totalmente satisfechos con haber podido proporcionar la mejor respuesta a las necesidades de Mutua Universal, aportando toda nuestra experiencia tanto en firma electrónica como en su aplicación dentro del ámbito sanitario donde se requiere máxima disponibilidad y facilidad de uso, y acompañarla en el avance de su proceso de Transformación Digital, mejorando la gestión de sus procesos internos y agilizando los trámites administrativos con los mutualistas y asociados”.

Mutua Universal implanta un servicio de firma en la nube con Grupo SIA

Gracias a esta iniciativa, la entidad obtiene una notable mejora en la eficiencia y ahorro de costes en los procesos internos, al tiempo que se garantiza la plena validez legal de la documentación contractual firmada.

Mutua Universal MUGENAT, Mutua Colaboradora con la Seguridad Social número 10, elegido a SIA (Sistemas Informáticos Abiertos), para poner en marcha un **sistema de firma digital en la nube que permite a la entidad evolucionar hacia una oficina digital y abordar sus procesos de una manera ágil y con plenas garantías legales** mediante firma electrónica cualificada bajo el reglamento eIDAS, equivalente a la firma manuscrita.

La propuesta de SIA cubre tanto los **servicios de emisión y gestión de los certificados cualificados como el uso de los mismos para la firma centralizada,** de manera integrada con sus aplicaciones de negocio y, por tanto, en completa movilidad -sin necesidad de ningún componente cliente instalado en el dispositivo del usuario-, o desde las aplicaciones de escritorio, mediante un agente software instalado en los puestos de trabajo para la autenticación y firma ante organismos oficiales.

Hace más de un año se implantó un sistema de firma biométrica y **ya se han firmado en esta modalidad casi dos millones de documentos y se dispone de 28 formularios integrados con la solución**, mejorando los tiempos de atención al paciente. “Con el impulso en el uso de certificados digitales eliminaremos el papel de nuestros procesos que requieren firma, sustituyendo la firma manuscrita mediante firma electrónica, con el fin de evolucionar hacia una oficina sin papel”, destaca Esther Felix, directora de Digitalización de Mutua Universal.

La entidad comenzó un proyecto para **dotar a los empleados de un certificado digital para 400 usuarios; quiso potenciar su uso y extenderlo hasta 2.500 usuarios** y a un mayor número de

procesos en los que se utilizan. Todo ello, mediante una plataforma cloud que aportase seguridad y confianza en entornos productivos de máxima exigencia, para lo cual SIA resultó adjudicataria del proyecto a través de licitación pública.
Además de la cobertura legal que ofrece SIA y la eliminación de las barreras tecnológicas que aporta la solución -firma en la nube sin necesidad de drivers ni instalación de agentes en sistemas finales-, los empleados de Mutua Universal "disponen a partir de ahora de todas las ventajas operativas y legales de la firma digital", según Marc Muntañá, director técnico de Control y Reporting de Mutua Universal.
Con el despliegue de la iniciativa, **la entidad logra ahorrar tiempo y costes en sus procesos internos** y contar con las garantías de seguridad jurídica que aporta el reglamento UE 910/2014 eIDAS mediante una plataforma tecnológica fácil de usar y respetuosa con el medio ambiente. Además, la solución proporcionará a los usuarios finales comodidad al evitar los desplazamientos, accesibilidad al firmar en cualquier momento y desde cualquier lugar y sencillez al realizar la firma desde cualquier dispositivo con acceso a internet.
Con esta y otras iniciativas, Mutua Universal sigue avanzando en su proceso de Innovación y Transformación Digital para responder a las necesidades actuales de sus asociados. La estrategia digital de la entidad sitúa a los mutualistas en el centro del proceso, con el objetivo de desarrollar soluciones con un beneficio práctico e inmediato para ellos.

Mutua Universal apuesta por la firma digital en nube de SIA

Mutua Universal ha elegido a SIA (Sistemas Informáticos Abiertos) para poner en marcha un sistema de firma digital en la nube que permite a la entidad evolucionar hacia una oficina digital y abordar sus procesos de una manera ágil y con plenas garantías legales mediante firma electrónica cualificada bajo el reglamento eIDAS, equivalente a la firma manuscrita.

La propuesta de SIA cubre tanto los servicios de emisión y gestión de los certificados cualificados como el uso de los mismos para la firma centralizada, de manera integrada con sus aplicaciones de negocio y, por tanto, en completa movilidad -sin necesidad de ningún componente cliente instalado en el dispositivo del usuario-, o desde las aplicaciones de escritorio, mediante un agente software instalado en los puestos de trabajo para la autenticación y firma ante organismos oficiales.

Hacia una oficina sin papel

Hace más de un año se implantó un sistema de firma biométrica y ya se han firmado en esta modalidad casi dos millones de documentos y se dispone de 28 formularios integrados con la solución, mejorando los tiempos de atención al paciente. “Con el impulso en el uso de certificados digitales eliminaremos el papel de nuestros procesos que requieren firma, sustituyendo la firma manuscrita mediante firma electrónica, con el fin de evolucionar hacia una oficina sin papel”, destaca Esther Felix, directora de Digitalización de Mutua Universal.

La entidad comenzó un proyecto para dotar a los

empleados de un certificado digital para 400 usuarios; quiso potenciar su uso y extenderlo hasta 2.500 usuarios y a un mayor número de procesos en los que se utilizan. Todo ello, mediante una plataforma cloud que aportase seguridad y confianza en entornos productivos de máxima exigencia, para lo cual SIA resultó adjudicataria del proyecto a través de licitación pública.

Además de la cobertura legal que ofrece SIA y la eliminación de las barreras tecnológicas que aporta la solución -firma en la nube sin necesidad de drivers ni instalación de agentes en sistemas finales-, los empleados de Mutua Universal "disponen a partir de ahora de todas las ventajas operativas y legales de la firma digital", según Marc Muntañá, director técnico de Control y Reporting de Mutua Universal.

Con el despliegue de la iniciativa de firma digital, Mutua Universal logra ahorrar tiempo y costes en sus procesos internos

Con el despliegue de la iniciativa de firma digital, la entidad logra ahorrar tiempo y costes en sus procesos internos y contar con las garantías de seguridad jurídica que aporta el reglamento UE 910/2014 eIDAS mediante una plataforma tecnológica fácil de usar y respetuosa con el medio ambiente. Además, la solución proporcionará a los usuarios finales comodidad al evitar los desplazamientos, accesibilidad al firmar en cualquier momento y desde cualquier lugar y sencillez al realizar la firma desde cualquier dispositivo con acceso a internet.

Con esta y otras iniciativas, Mutua Universal sigue avanzando en su proceso de Innovación y Transformación Digital para responder a las necesidades actuales de sus asociados. La estrategia digital de la entidad sitúa a los mutualistas en el centro del proceso, con el objetivo de desarrollar soluciones con un beneficio práctico e inmediato para ellos.

Tecnología de confianza y conocimiento experto

El éxito del proyecto ha residido en tres pilares fundamentales: la cualificación eIDAS de los servicios que presta SIA a través de SIACERT TrustedServices; los máximos niveles de seguridad y certificación de la tecnología de SIAVAL SafeCert, utilizada para la firma en la nube y certificada como dispositivo cualificado de

creación de firma (QSCD) a nivel europeo; y, como apunta Muntañá, “la combinación de la experiencia, alto conocimiento y desempeño de sus profesionales en el desarrollo de proyectos similares en el ámbito de la Firma Electrónica, tanto desde un punto de vista técnico como legal, y de la facilidad de implantación de la solución por parte del equipo de Digitalización y Tecnología de Mutua Universal”.

Por su parte, Alfonso Fernández, director de Desarrollo de Negocio en SIA, señala que “estamos totalmente satisfechos con haber podido proporcionar la mejor respuesta a las necesidades de Mutua Universal, aportando toda nuestra experiencia tanto en firma digital como en su aplicación dentro del ámbito sanitario donde se requiere máxima disponibilidad y facilidad de uso, y acompañarla en el avance de su proceso de Transformación Digital, mejorando la gestión de sus procesos internos y agilizando los trámites administrativos con los mutualistas y asociados”.

elEconomista.es

4 Abril 2019

Mutua Universal impulsa su transformación digital con el servicio de firma en la nube de SIA

La entidad obtiene una notable mejora en la eficiencia y ahorro de coste

Mutua Universal MUGENAT, Mutua Colaboradora con la Seguridad Social número 10, ha elegido a SIA (Sistemas Informáticos Abiertos), proveedor líder de soluciones de seguridad y servicios de administración de TI, para poner en marcha un sistema de firma digital en la nube que permite a la entidad evolucionar hacia una oficina digital y abordar sus procesos de una manera ágil y con plenas garantías legales mediante firma electrónica cualificada bajo el reglamento eIDAS, equivalente a la firma manuscrita.

La propuesta de SIA cubre tanto los servicios de emisión y gestión de los certificados cualificados como el uso de los mismos para la firma centralizada, de manera integrada con sus aplicaciones de negocio y, por tanto, en completa movilidad -sin necesidad de ningún componente cliente instalado en el dispositivo del usuario-, o desde las aplicaciones de escritorio, mediante un agente software instalado en los puestos de trabajo para la autenticación y firma ante organismos oficiales.

Hacia una oficina sin papel

Hace más de un año se implantó un sistema de firma biométrica y ya se han firmado en esta modalidad casi dos

millones de documentos y se dispone de 28 formularios integrados con la solución, mejorando los tiempos de atención al paciente. "Con el impulso en el uso de certificados digitales eliminaremos el papel de nuestros procesos que requieren firma, sustituyendo la firma manuscrita mediante firma electrónica, con el fin de evolucionar hacia una oficina sin papel", destaca Esther Felix, directora de Digitalización de Mutua Universal.

La entidad comenzó un proyecto para dotar a los empleados de un certificado digital para 400 usuarios; quiso potenciar su uso y extenderlo hasta 2.500 usuarios y a un mayor número de procesos en los que se utilizan. Todo ello, mediante una plataforma cloud que aportase seguridad y confianza en entornos productivos de máxima exigencia, para lo cual SIA resultó adjudicataria del proyecto a través de licitación pública.

Además de la cobertura legal que ofrece SIA y la eliminación de las barreras tecnológicas que aporta la solución -firma en la nube sin necesidad de drivers ni instalación de agentes en sistemas finales-, los empleados de Mutua Universal "disponen a partir de ahora de todas las ventajas operativas y legales de la firma digital", según Marc Muntañá, director técnico de Control y Reporting de Mutua Universal.

Con el despliegue de la iniciativa, la entidad logra ahorrar tiempo y costes en sus procesos internos y contar con las garantías de seguridad jurídica que aporta el reglamento UE 910/2014 eIDAS mediante una plataforma tecnológica fácil de usar y respetuosa con el medio ambiente. Además, la solución proporcionará a los usuarios finales comodidad al evitar los desplazamientos, accesibilidad al firmar en cualquier momento y desde cualquier lugar y sencillez al realizar la firma desde cualquier dispositivo con acceso a Internet.

Con esta y otras iniciativas, Mutua Universal sigue avanzando en su proceso de Innovación y Transformación Digital para responder a las necesidades actuales de sus asociados. La estrategia digital de la entidad sitúa a los mutualistas en el centro del proceso, con el objetivo de desarrollar soluciones con un beneficio práctico e inmediato para ellos.

Tecnología de confianza y conocimiento experto

El éxito del proyecto ha residido en tres pilares fundamentales: la cualificación eIDAS de los servicios que presta SIA a través de

SIACERT TrustedServices; los máximos niveles de seguridad y certificación de la tecnología de SIAVAL SafeCert, utilizada para la firma en la nube y certificada como dispositivo cualificado de creación de firma (QSCD) a nivel europeo; y, como apunta Muntañá, "la combinación de la experiencia, alto conocimiento y desempeño de sus profesionales en el desarrollo de proyectos similares en el ámbito de la Firma Electrónica, tanto desde un punto de vista técnico como legal, y de la facilidad de implantación de la solución por parte del equipo de Digitalización y Tecnología de Mutua Universal".

Por su parte, Alfonso Fernández, director de Desarrollo de Negocio en SIA, señala que "estamos totalmente satisfechos con haber podido proporcionar la mejor respuesta a las necesidades de Mutua Universal, aportando toda nuestra experiencia tanto en firma electrónica como en su aplicación dentro del ámbito sanitario donde se requiere máxima disponibilidad y facilidad de uso, y acompañarla en el avance de su proceso de Transformación Digital, mejorando la gestión de sus procesos internos y agilizando los trámites administrativos con los mutualistas y asociados".

Cifras

Ranking 2019

PUESTO 2018	EMPRESA	FACTURACIÓN 2018		FACTURACIÓN 2017	VARIACIÓN %	PLANTILLA 2018	PLANTILLA 2017	VARIACIÓN %
	AtSistemas	58 €		45,50 €	27,47%	1209	954	26,73%
60	Compusof	56 €	*CW	53 €	5,66%	600	600	99,54%
61	Acens	52,70 €		48 €	9,79%	243	244	-0,41%
62	Grupo CMC	51,50 €		36,37 €	41,60%	1000	820	21,95%
63	Equinix	51 €	*CW	49,50 €	3,03%	200	226	-11,50%
64	Satlink	50,30 €		48 €	4,79%	50	48	4,17%
65	Sistemas Informáticos Abiertos (SIA)	47,80 €		41,04 €	16,47%	646	557	15,98%
66	Abast	45,30 €		41 €	10,49%	480	450	6,67%
67	Atmira	45 €		40 €	12,50%	826	750	10,13%
68	Izertis	39,50 €		25,63 €	54,12%	637	452	40,93%
69	Sogeti	39,45 €	*CW	28,67 €	37,60%	700	627	11,64%
70	Meta4	37 €		33 €	12,12%	563	530	6,23%
71	Grupo Costaisa	36,75 €		35,86 €	2,48%	331	316	4,75%
72	Omega Peripherals	33 €		38 €	-13,16%	130	115	13,04%
73	Interxion	32 €	*CW	30 €	6,67%	30	26	15,38%
74	BABEL	31,60 €		26,50 €	19,25%	670	560	19,64%
75	Singular People	30 €		20 €	50,00%	568	420	35,24%
	Devoteam	30 €		25 €	20,00%	583	500	16,60%
77	Mnemo Evolution & Integration Services	29 €		27 €	6,18%	518	510	1,57%
78	Aryan Comunicaciones	27 €		25 €	8,16%	65	64	1,56%
79	Ingecom	25 €		23 €	8,68%	29	24	20,83%

Las cifras de facturación son en millones de euros y para el mercado español | *CW: estimaciones realizadas por ComputerWorld | *: estimaciones realizadas por la propia compañía

SEGURI PRESS

Mayte Carvajal, nueva responsable de Administración y Compras de Magal

Magal anunció, el 6 de marzo, la incorporación de **Mayte Carvajal** como nueva responsable de Administración y Compras.

Graduada superior en dirección y administración de empresas, multilingüe y con amplio bagaje en gestión y dirección de compras, Carvajal cuenta con diez años de experiencia en Pullmantur, donde ha ocupado distintos cargos relacionados con su especialidad.

Anteriormente trabajó cinco años como consultora *freelance* de compras y aprovisionamientos en Marruecos, por lo que también se maneja en el mercado norteafricano.

En definitiva, según Miguel Ángel López, director de la compañía en la península, "con esta incorporación queremos dar a nuestras compras y contrataciones la trascendencia y profesionalización que merecen como parte esencial del compromiso excepcional que mantenemos con nuestros clientes".

www.ms3.es

El CCN se incorpora al Charter of Trust para fomentar la ciberseguridad

El Charter of Trust, organismo impulsado por Siemens cuyo objetivo es fomentar la ciberseguridad a través de cadenas de suministro globales, cuenta con el Centro Criptológico Nacional (CCN) como nuevo miembro asociado. De la misma manera, también se han unido con esta categoría la Oficina Federal Alemana para la Seguridad de la Información y la Universidad Tecnológica de Graz (Austria).

El miembro asociado es un nuevo formato a través del cual el Charter of Trust está abriéndose para cooperar con representantes gubernamentales importantes, universidades y grupos de reflexión. El beneficio para estas organizaciones es la cooperación en proyectos específicos sin tener que ser miembros plenos con todos sus derechos y responsabilidades.

www.siemens.com

Antidroga@policia.es recibió 15.000 correos a lo largo del año

Durante 2018, la dirección de correo electrónico antidroga@policia.es recibió más de 40 informaciones diarias relacionadas con la lucha contra el tráfico de narcóticos. La eficacia de esta herramienta de colaboración ciudadana ha aumentado con la recepción de 15.000 *emails*, 5.000 más que en 2017, que fueron analizados minuciosamente por especialistas de la Brigada Central de Estupefacientes de la **Policía Nacional**.

Desde la puesta en marcha de la dirección antidroga@policia.es, en 2012, se han recibido más de 68.000 informaciones. Y gracias a ellas ha sido posible descubrir puntos negros de venta, investigaciones sobre narcotraficantes, aprehender plantaciones de marihuana, tablecimientos de ocio donde se distribuían sustancias estupefacientes.

Entre otras actuaciones destacadas, la información facilitada a través de [illegible] tió aprehender 277 kilos de cocaína en el puerto de Barcelona en 2013. [illegible] incautaron cinco toneladas de hachís en la operación Costa-Bahía-Jaitan y [illegible] la operación Cora, se intervinieron 429 kilos de cocaína y se desarticuló [illegible] de venta de drogas en Internet. En 2017 también se aprehendieron 552 [illegible] 2018 se detuvieron a cinco personas pertenecientes a un grupo de narcotráfico.

Para más información: www.policia.es

SIA amplía su propuesta de soluciones de continuidad de negocio con Everbridge

SIA (Sistemas Informáticos Abiertos) y Everbridge han firmado un acuerdo como socios para ofrecer a las empresas los beneficios de las soluciones unificadas que componen la plataforma de la propia Everbridge.

Con esta alianza, SIA incorpora a su oferta la plataforma de gestión de eventos críticos de Everbridge –que permite garantizar la seguridad de las personas y edificios de una organización para la continuidad del negocio– y la solución IT-Alerting, que posibilita evaluar, mitigar y reducir el impacto de cualquier ciberincidente. De este modo, ofrece una solución integral para abordar los desafíos de la seguridad y continuidad del negocio.

Para más información: www.sia.es

El proyecto Ocean Master en los premios FINE [illegible] un dron submarino

El proyecto Ocean Master [illegible] modo por Elmco, Aussa, [illegible] y con Navantia como [illegible] fado ganador en la categoría [illegible] genería marítima destacada [illegible] FINE para el Fomento de la [illegible] Española. El jurado tuvo en [illegible] vación en la construcción y [illegible] las mejoras y beneficios que [illegible]

En concreto, el proyecto [illegible] tónomo multipropósito para [illegible] tes y roles en operaciones de [illegible] tiene la capacidad de realizar [illegible] bientes altamente complejos.

Para más información: www.electronico-[illegible]

La Junta de Andalucía gestionó más de 8.100 ciberincidentes en [illegible] más que el año anterior

La **Junta de Andalucía** atendió, a través del centro de respuesta a incidentes de ciberseguridad Andalucía-CERT, más de 8.100 incidentes en 2018, la mayoría de ellos relacionados con código dañino, fraude e intrusiones.

En comparación con el año anterior, el número de casos gestionados se incrementó un 32 por ciento debido al aumento de los ataques en la Red, a la mejora continua en [illegible] tección del centro y al mejor conocimiento de los procedimientos de notificación por parte del personal de la administración pública andaluza.

Para más información: www.juntadeandalucia.es

SIA amplía su propuesta de soluciones de continuidad de negocio con Everbridge

SIA (Sistemas Informáticos Abiertos) y Everbridge han firmado un acuerdo como socios para ofrecer a las empresas los beneficios de las soluciones unificadas que componen la plataforma de la propia Everbridge.

Con esta alianza, SIA incorpora a su oferta la plataforma de gestión de eventos críticos de Everbridge –que permite garantizar la seguridad de las personas y edificios de una organización para la continuidad del negocio– y la solución IT-Alerting, que posibilita evaluar, mitigar y reducir el impacto de cualquier ciberincidente. De este modo, ofrece una solución integral para abordar los desafíos de la seguridad y continuidad del negocio.

Para más información: www.sia.es

computing

12 Abril 2019

Grupo SIA incrementa su facturación en un 22% hasta los 57 millones de euros

El grupo, que opera en España y Portugal, alcanzó también un EBITDA superior a los 5 millones de euros.

Grupo SIA (Sistemas Informáticos Abiertos), proveedor de soluciones de seguridad y servicios de administración de TI, ha cerrado el ejercicio fiscal 2018 con una **facturación de 57 millones de euros**, lo que supone un crecimiento del 22% con respecto al año anterior. El grupo, que opera en España y Portugal, alcanzó también un EBITDA superior a los 5 millones de euros.

“Estos resultados confirman la tendencia del crecimiento de doble dígito de los ingresos y el EBITDA de los últimos años como resultado de la expansión del **mercado de ciberseguridad, la inversión en tecnología propia de Firma Digital en la nube** y las iniciativas de transformación que han formado parte de nuestro plan de negocio 2014-2018”, apunta **Enrique Palomares, CEO del Grupo SIA**. La evolución de los resultados del grupo se basa fundamentalmente, según explica la propia compañía, "en la labor del equipo profesional de expertos acreditados que lo conforma, con amplia experiencia y conocimiento en cada ámbito tecnológico". **Durante 2018, la plantilla de SIA ha crecido un 14%** y, en la actualidad, cuenta con más de 700 personas entre ambas geografías.

La compañía, en este sentido, afirma continuar su compromiso de fomentar la creación de empleo cualificado y estable y la formación de sus profesionales. Los esfuerzos se centran en identificar y desarrollar el potencial de las personas, con el fin de ofrecer oportunidades de carrera y orientar el desempeño a dar el mejor servicio a sus clientes.

En este sentido, cabe destacar, por un lado, que SIA cuenta entre sus filas con 212 personas con certificaciones, sumando

un total de 534 en vigor; y, por otro, su apuesta por la incorporación de perfiles junior con vocación STEM (disciplinas académicas de Ciencia, Tecnología, Ingeniería y Matemáticas); el año pasado, 30 jóvenes de los 34 que finalizaron sus prácticas en la compañía, eligieron continuar en SIA su carrera profesional.

Los resultados alcanzados en cada una de las divisiones de negocio del grupo representan un 20% en Consultoría, un 56% en Infraestructuras y Proyectos y un 24% en Cloud & Servicios Profesionales.

Por industrias, la compañía tiene presencia en todos los sectores de actividad distribuida de la siguiente manera: un 22% en Administraciones Públicas y Sanidad, un 24% en Banca y Seguros, un 14% en Industria y Servicios y un 40% en Telco y Media.

Expansión

12 Abril 2019

Incorpora al presidente de Mercedes-Benz en España a su consejo de administración

Revés judicial en Francia

La facturación aumentó un 22%

Carole Ghosn niega su implicación en el presunto enriquecimiento de su marido

El fiasco de Lyft rebaja la ambición de Uber en su salida a Bolsa

La facturación aumentó un 22%

GRUPO SIA El proveedor de soluciones de seguridad y servicios de administración de TI facturó 57 millones de euros el año pasado, un 22% más que en 2017. El grupo, que opera en España y Portugal, alcanzó también un ebitda superior a los 5 millones de euros.

Grupo SIA incrementa su facturación en un 22% hasta los 57 millones de euros

Grupo SIA, Sistemas Informáticos Abiertos, ha cerrado el ejercicio fiscal 2018 (del 1 de enero al 31 de diciembre de 2018) con una facturación de 57 millones de euros, lo que supone un crecimiento del 22% con respecto al año anterior. El grupo, que opera en España y Portugal, alcanzó también un EBITDA superior a los 5 millones de euros.

"Estos resultados confirman la tendencia del crecimiento de doble dígito de los ingresos y el EBITDA de los últimos años como resultado de la expansión del mercado de Ciberseguridad, la inversión en tecnología propia de Firma Digital en la nube y las iniciativas de transformación que han formado parte de nuestro plan de negocio 2014-2018", apunta Enrique Palomares, CEO del Grupo SIA. La evolución de los resultados del grupo se basa fundamentalmente en la labor del equipo profesional de expertos acreditados que lo conforma, con amplia experiencia y conocimiento en cada ámbito tecnológico.

Durante 2018, la plantilla de SIA ha crecido un 14% y, en la actualidad, cuenta con más de 700 personas entre ambas geografías.

La compañía, en este sentido, continúa su compromiso de fomentar la creación de empleo cualificado y estable y la formación de sus profesionales. Los esfuerzos se centran principalmente en identificar y desarrollar el potencial de las personas, con el fin de ofrecer oportunidades de carrera y orientar el desempeño a dar el mejor servicio a sus clientes.

En este sentido, cabe destacar, por un lado, que SIA cuenta entre sus filas con 212 personas con certificaciones, sumando un total de 534 en vigor; y, por otro, su apuesta por la incorporación de perfiles junior con vocación STEM (disciplinas académicas de Ciencia, Tecnología, Ingeniería y Matemáticas); el año pasado, 30 jóvenes de los 34 que finalizaron sus prácticas en la compañía, eligieron continuar en SIA su carrera profesional.

Los resultados alcanzados en cada una de las divisiones de negocio del grupo representan un 20% en Consultoría, un 56% en Infraestructuras y Proyectos y un 24% en Cloud &

Servicios Profesionales.
Por industrias, la compañía tiene presencia en todos los sectores de actividad distribuida de la siguiente manera: un 22% en Administraciones Públicas y Sanidad, un 24% en Banca y Seguros, un 14% en Industria y Servicios y un 40% en Telco y Media.

Grupo SIA incrementa su facturación en un 22%

Grupo SIA ha cerrado el ejercicio fiscal 2018 (del 1 de enero al 31 de diciembre de 2018) con una facturación de 57 millones de euros, lo que supone un crecimiento del 22% con respecto al año anterior. El grupo, que opera en España y Portugal, alcanzó también un EBITDA superior a los 5 millones de euros.

"Estos resultados confirman la tendencia del crecimiento de doble dígito de los ingresos y el EBITDA de los últimos años como resultado de la expansión del mercado de Ciberseguridad, la inversión en tecnología propia de Firma Digital en la nube y las iniciativas de transformación que han formado parte de nuestro plan de negocio 2014-2018", apunta Enrique Palomares, CEO del Grupo SIA.

La evolución de los resultados del grupo se basa fundamentalmente en la labor del equipo profesional de expertos acreditados que lo conforma, con amplia experiencia y conocimiento en cada ámbito tecnológico. Durante 2018, la plantilla de SIA ha crecido un 14% y, en la actualidad, cuenta con más de 700 personas entre ambas geografías.

La compañía, en este sentido, continúa su compromiso de fomentar la creación de empleo cualificado y estable y la formación de sus profesionales. Los esfuerzos se centran principalmente en identificar y desarrollar el potencial de

las personas, con el fin de ofrecer oportunidades de carrera y orientar el desempeño a dar el mejor servicio a sus clientes.

Grupo SIA cuenta entre sus filas con 212 personas con certificaciones, sumando un total de 534 en vigor

En este sentido, cabe destacar, por un lado, que Grupo SIA cuenta entre sus filas con 212 personas con certificaciones, sumando un total de 534 en vigor; y, por otro, su apuesta por la incorporación de perfiles junior con vocación STEM (disciplinas académicas de Ciencia, Tecnología, Ingeniería y Matemáticas); el año pasado, 30 jóvenes de los 34 que finalizaron sus prácticas en la compañía, eligieron continuar en SIA su carrera profesional.

Los resultados alcanzados en cada una de las divisiones de negocio del grupo representan un 20% en Consultoría, un 56% en Infraestructuras y Proyectos y un 24% en Cloud & Servicios Profesionales.

redseguridad.com

17 Abril 2019

Grupo SIA crece un 22% en 2018 y factura 57 millones de euros

El mercado español sigue representando la principal fuente de crecimiento del grupo, con unos ingresos de 48 millones de euros.

El proveedor de soluciones de seguridad y servicios de administración de TI, Grupo SIA (Sistemas Informáticos Abiertos), ha cerrado el ejercicio fiscal 2018, que va del 1 de enero al 31 de diciembre de 2018, con una facturación de **57 millones de euros**, lo que supone un **crecimiento del 22%** con respecto al año anterior. El grupo, que opera en España y Portugal, alcanzó también **un EBITDA superior a los 5 millones de euros**.

En palabras de Enrique Palomares, CEO de la compañía, "estos resultados confirman la tendencia del crecimiento de doble dígito de los ingresos y el EBITDA de los últimos años como resultado de la **expansión del mercado de ciberseguridad**, la inversión en tecnología propia de **firma digital en la nube** y las **iniciativas de transformación** que han formado parte de nuestro plan de negocio 2014-2018".

El mercado español sigue representando la principal fuente de crecimiento del grupo. En el ejercicio fiscal 2018 alcanzó una facturación cercana a los 48 millones de euros, lo que significa un aumento del 22% frente al año anterior. Por su parte, en el mercado portugués, Grupo SIA opera a través de la marca CESCE SI, proveedor de soluciones de almacenamiento de datos que adquirió en 2004. CESCE cerró el ejercicio fiscal con una cifra de

negocio de **9,4 millones de euros**, lo que supone un **incremento del 25%** con respecto a 2017.

La evolución de los resultados del grupo se basa, a juicio de la empresa, en **la labor de su equipo de profesionales**, con amplia experiencia y conocimiento en cada ámbito tecnológico, y que durante 2018 **creció un 14%** hasta conformar su actual plantilla, la cual supera **las 700 personas**. La empresa, además, apuesta por la formación de sus profesionales. En este sentido, cuenta entre sus filas con 212 personas con certificaciones, sumando un total de 534 en vigor. Además, subraya su compromiso por la incorporación de **perfiles junior con vocación STEM** (disciplinas académicas de Ciencia, Tecnología, Ingeniería y Matemáticas). De hecho, el año pasado, 30 jóvenes de los 34 que finalizaron sus prácticas en la compañía eligieron continuar en SIA su carrera profesional.

Finalmente, y abordando la facturación por divisiones, **Consultoría** representó el **20%**, **Infraestructuras y Proyectos**, el **56%**; y **Cloud & Servicios Profesionales**, el **24%**. Por industrias, la compañía tiene presencia en todos los sectores de actividad distribuida de la siguiente manera: un **22%** en **Administraciones Públicas y Sanidad**, un **24%** en **Banca y Seguros**, un **14%** en **Industria y Servicios** y un **40%** en **Telco y Media**.

Se puede acceder a un resumen infográfico de los resultados de la compañía en este enlace.

Sistema de firma digital

Por otro lado, la empresa ha hecho público también la implantación de un sistema de **firma digital en la nube** en su cliente **Mutua Universal MUGENAT**, Mutua Colaboradora con la Seguridad Social número 10. Esto permitirá a la entidad evolucionar hacia una **oficina digital** y abordar sus procesos de una manera ágil y con plenas garantías legales mediante firma electrónica cualificada bajo el **reglamento eIDAS**, equivalente a la firma manuscrita.

En este sentido, la propuesta de SIA cubre tanto los servicios de emisión y gestión de los certificados cualificados, como el uso de los mismos para la firma centralizada. Además, se produce de manera **integrada**

con sus aplicaciones de negocio y, por tanto, en completa movilidad; o desde las aplicaciones de escritorio, mediante un agente software instalado en los puestos de trabajo para la autenticación y firma ante organismos oficiales.

"Con el impulso en el uso de certificados digitales eliminaremos el papel de nuestros procesos que requieren firma, sustituyendo la manuscrita por la electrónica, con el fin de evolucionar hacia **una oficina sin papel**", comenta Esther Felix, directora de Digitalización de Mutua Universal.

De esta forma, con el despliegue de la iniciativa, la entidad logra **ahorrar tiempo y costes** en sus procesos internos y contar con las **garantías de seguridad jurídica** que aporta el reglamento UE 910/2014 eIDAS mediante una plataforma tecnológica fácil de usar y respetuosa con el medio ambiente. Además, la solución proporcionará a los usuarios finales **comodidad** al evitar los desplazamientos, **accesibilidad** al firmar en cualquier momento y desde cualquier lugar, y **sencillez** al realizar la firma desde cualquier dispositivo con acceso a Internet.

2 Mayo 2019

Baleares recurre seguridad del

IB-Salut ha logrado optimizar el día a día de sus más de 18.000 profesionales y, a su vez, mejorar el servicio a los ciudadanos, alcanzando altos niveles de eficiencia y eficacia en términos de seguridad, de tiempo, de costes y cumplimiento legal.

El servicio de Salud de Baleares recurre a SIA para garantizar la seguridad del acceso a sus TI

El servicio de Salud de Baleares recurre a SIA para garantizar la seguridad del acceso a sus TI

El servicio de Salud de Baleares recurre a SIA para garantizar la seguridad del acceso a sus TI

El Servicio de Salud de las Islas Baleares (IB-Salut) ha depositado su confianza, una vez más, en SIA (Sistemas Informáticos Abiertos), proveedor líder de seguridad y servicios de administración de TI, para abordar la evolución de su sistema de Gestión de Identidades (GID) a través de la actualización de la versión desplegada, dotando a la plataforma del soporte profesional necesario y de nuevas funcionalidades.

El sistema de Gestión de Identidades de que dispone el organismo balear aborda la gestión de la identificación y el control de acceso de sus profesionales a la información y se implementó en torno a un modelo de roles y responsabilidades que unifica el acceso a los Sistemas de Información de atención primaria (159 centros de salud) y de atención especializada (diez hospitales) y un autoservicio de provisión de identidades para facilitar la movilidad entre los centros.

Este sistema permite que el personal de IB-Salut se encuentre localizado organizativamente de modo adecuado y los permisos que se le atribuyen tengan una correspondencia directa con el rol laboral que desempeñan en todo momento.

"Nuestra vocación de servicio público ha sido y es el eje central de las mejoras tecnológicas emprendidas en el IB-Salut; gracias a este proyecto, nuestros profesionales pueden disponer de acceso inmediato a los Sistemas de Información que necesitan para el ejercicio de sus funciones, desde el momento de su incorporación al organismo, lo que garantiza que los ciudadanos disfruten de una correcta y completa atención asistencial", apunta Miguel Ángel Benito, jefe del Servicio de Seguridad de la Información en IB-Salut.

Entre otras cuestiones, la actualización del sistema de GID ha logrado mejorar las comunicaciones a los usuarios, el cumplimiento normativo (RGPD y Esquena Nacional de Seguridad), la gestión de credenciales privilegiadas de administradores y ha incorporado el portal de autoservicio de GID (IBSalut-Store), a través del cual los profesionales pueden solicitar el acceso a aquellos sistemas que no se le han asignado por regla de negocio según su perfil.

Se trata de un único portal y procedimiento para la solicitud de permisos que logra eliminar los desplazamientos de los profesionales, simplificar la tarea de aprobación de las solicitudes, asignar automáticamente los permisos y ofrecer la trazabilidad de las autorizaciones de permisos a acceso. Además, entre otros recursos, IBSalut-Store permite acceder al certificado electrónico centralizado, que posibilita autenticarse y firmar documentos electrónicos desde cualquier dispositivo con acceso a internet y sin equipamiento adicional.

Con motivo de la puesta en marcha del servicio de firma centralizada en el Servicio de Salud de las Islas Baleares, también de la mano de SIA, se ha integrado el sistema de GID con la Autoridad de Certificación de SIA. Esta integración, que supone la gestión de la solicitud del certificado por parte del profesional, aprobación o rechazo de la solicitud desde el área de Recursos Humanos y la revocación del certificado, ha conseguido reducir de 25 minutos a cinco el tiempo de emisión de certificados en el área de RR.HH. y de 120 a 5 en atención primaria; la revocación inmediata de los certificados de empleado público; y la trazabilidad de los emitidos.

Según señala Alfonso Fernández, director de Desarrollo de

Servicio de Salud de las Islas Baleares desde hace años en esta y otras iniciativas nos ha ayudado a entender sus necesidades de forma más efectiva para poder facilitarle así la solución más adecuada. Los resultados alcanzados avalan una vez más la idoneidad de la propuesta tecnológica de SIA".

El proyecto, que ha alcanzado la tramitación de 500 solicitudes de permisos y 3.000 solicitudes de certificado centralizado desde octubre de 2018, dota al profesional de una única credencial/contraseña, de acceso inmediato a los sistemas desde la contratación, implanta sistemas de recuperación rápida de contraseñas, incorpora al ciclo de vida de la identidad la gestión del certificado electrónico centralizado y da respuesta a los requerimientos legales.

El resultado final es un sistema que incrementa la seguridad y la productividad, a la vez que disminuye costes y el esfuerzo redundante en aras del ciudadano, un paso más hacia delante de la Administración Pública balear en la modernización de la prestación del servicio sanitario a través de las Tecnologías de la Información.

computing

3 Mayo 2019

Islas Baleares garantiza la seguridad de su Salud

IB-Salut ha logrado optimizar junto con SIA el día a día de sus más de 18.000 profesionales.

El Servicio de Salud de las Islas Baleares (IB-Salut) ha depositado su confianza, una vez más, en SIA (Sistemas Informáticos Abiertos), proveedor de seguridad y servicios de administración de TI, para abordar la evolución de su sistema de Gestión de Identidades (GID) a través de la actualización de la versión desplegada, dotando a la plataforma del soporte profesional necesario y de nuevas funcionalidades.

El sistema de Gestión de Identidades de que dispone el organismo balear aborda la gestión de la identificación y el control de acceso de sus profesionales a la información y se implementó en torno a un modelo de roles y responsabilidades que unifica el acceso a los Sistemas de Información de atención primaria (159 centros de salud) y de atención especializada (diez hospitales) y un autoservicio de provisión de identidades para facilitar la movilidad entre los centros.

> El sistema de Gestión de Identidades de que dispone el organismo balear aborda la gestión de la identificación y el control de acceso de sus profesionales a la información

Este sistema permite que el personal de IB-Salut se encuentre localizado organizativamente de modo adecuado y los permisos que se le atribuyen tengan una correspondencia directa con el rol laboral que desempeñan en todo momento.

“Nuestra vocación de servicio público ha sido y es el eje central de las mejoras tecnológicas emprendidas en el IB-Salut; gracias a este proyecto, nuestros profesionales pueden disponer de acceso inmediato a los Sistemas de Información que necesitan para el ejercicio de sus funciones, desde el momento de su

incorporación al organismo, lo que garantiza que los ciudadanos disfruten de una correcta y completa atención asistencial", apunta Miguel Ángel Benito, jefe del Servicio de Seguridad de la Información en IB-Salut.

Entre otras cuestiones, la actualización del sistema de GID ha logrado mejorar las comunicaciones a los usuarios, el cumplimiento normativo (RGPD y Esquena Nacional de Seguridad), la gestión de credenciales privilegiadas de administradores y ha incorporado el portal de autoservicio de GID (IBSalut-Store), a través del cual los profesionales pueden solicitar el acceso a aquellos sistemas que no se le han asignado por regla de negocio según su perfil.

Se trata de un único portal y procedimiento para la solicitud de permisos que logra eliminar los desplazamientos de los profesionales, simplificar la tarea de aprobación de las solicitudes, asignar automáticamente los permisos y ofrecer la trazabilidad de las autorizaciones de permisos a acceso. Además, entre otros recursos, IBSalut-Store permite acceder al certificado electrónico centralizado, que posibilita autenticarse

y firmar documentos electrónicos desde cualquier dispositivo con acceso a internet y sin equipamiento adicional.

Con motivo de la puesta en marcha del servicio de firma centralizada en el Servicio de Salud de las Islas Baleares,

también de la mano de SIA, se ha integrado el sistema de GID con la Autoridad de Certificación de SIA. Esta integración, que supone la gestión de la solicitud del certificado por parte del profesional, aprobación o rechazo de la solicitud desde el área de Recursos Humanos y la revocación del certificado, ha conseguido reducir de 25 minutos a cinco el tiempo de emisión de certificados en el área de RR.HH. y de 120 a 5 en atención primaria; la revocación inmediata de los certificados de empleado público; y la trazabilidad de los emitidos.

Según señala Alfonso Fernández, director de Desarrollo de Negocio en SIA, “la colaboración que mantenemos con el Servicio de Salud de las Islas Baleares desde hace años en esta y otras iniciativas nos ha ayudado a entender sus necesidades de forma más efectiva para poder facilitarle así la solución más adecuada. Los resultados alcanzados avalan una vez más la idoneidad de la propuesta tecnológica de SIA”.

El proyecto

El proyecto, que ha alcanzado la tramitación de 500 solicitudes de permisos y 3.000 solicitudes de certificado centralizado desde octubre de 2018, dota al profesional de una única credencial/contraseña, de acceso inmediato a los sistemas desde la contratación, implanta sistemas de recuperación rápida de contraseñas, incorpora al ciclo de vida de la identidad la gestión del certificado electrónico centralizado y da respuesta a los requerimientos legales.

El resultado final es un sistema que incrementa la seguridad y la productividad, a la vez que disminuye costes y el esfuerzo redundante en aras del ciudadano, un paso más hacia delante de la Administración Pública balear en la modernización de la prestación del servicio sanitario a través de las Tecnologías de la Información.

El servicio de Salud de Baleares garantiza con SIA la seguridad en el acceso a sus sistemas de Información

A través de esta iniciativa, desarrollada por SIA, el Servicio de Salud de las Islas Baleares ha logrado optimizar el día a día de sus más de 18.000 profesionales y mejorar el servicio a los ciudadanos, alcanzando altos niveles de eficiencia y eficacia en términos de seguridad, tiempo, costes y cumplimiento legal.

El **Servicio de Salud de las Islas Baleares (IB-Salut)** ha depositado su confianza, una vez más, en SIA (Sistemas Informáticos Abiertos), proveedor líder de seguridad y servicios de administración de TI, para abordar la evolución de su sistema de Gestión de Identidades (GID) a través de la actualización de la versión desplegada, dotando a la plataforma del soporte profesional necesario y de nuevas funcionalidades.

El sistema de **Gestión de Identidade**s de que dispone el organismo balear aborda la gestión de la identificación y el control de acceso de sus profesionales a la información y se implementó en torno a un modelo de roles y responsabilidades que unifica el acceso a los Sistemas de Información de atención primaria (159 centros de salud) y de atención especializada (diez hospitales) y un autoservicio de provisión de identidades para facilitar la movilidad entre los centros.

Mejor comunicación con los usuarios

Este sistema permite que el personal de IB-Salut se encuentre **localizado organizativamente** de modo adecuado y los permisos que se le atribuyen tengan una correspondencia directa con el rol laboral que desempeñan en todo momento. "*Nuestra vocación de servicio público ha sido y es el eje central de las mejoras tecnológicas emprendidas en el IB-Salut; gracias a este proyecto, nuestros profesionales pueden disponer de acceso inmediato a los Sistemas de Información que necesitan para el ejercicio de sus funciones, desde el momento de su incorporación al organismo, lo que garantiza que los ciudadanos disfruten de una correcta y*.

completa atención asistencial", apunta **Miguel Ángel Benito**, jefe del Servicio de Seguridad de la Información en IB-Salut.

Entre otras cuestiones, la actualización del sistema de GID ha logrado mejorar las comunicaciones a los usuarios, el cumplimiento normativo (RGPD y Esquena Nacional de Seguridad), la gestión de credenciales privilegiadas de administradores y ha incorporado el portal de autoservicio de GID (IBSalut-Store), a través del cual los profesionales pueden solicitar el acceso a aquellos sistemas que no se le han asignado por regla de negocio según su perfil.

Portal único

Se trata de un **único portal y procedimiento para la solicitud de permisos** que logra eliminar los desplazamientos de los profesionales, simplificar la tarea de aprobación delas solicitudes, asignar automáticamente los permisos y ofrecer la trazabilidad de las autorizaciones de permisos a acceso.Además, entre otros recursos, IBSalut-Store permite acceder al certificado electrónico centralizado, que posibilita autenticarse y. firmar documentos electrónicos desde cualquier dispositivo con acceso a internet y sin equipamiento adicional.

Con motivo de la puesta en marcha del servicio de firma centralizada en el Servicio de Salud de las Islas Baleares, también de la mano de SIA, se ha **integrado el sistema de GID con la Autoridad de Certificación de SIA.**

Esta integración, que supone la gestión de la solicitud del certificado por parte del profesional, aprobación o rechazo de la solicitud desde el área de Recursos Humanos y la revocación del certificado, ha conseguido reducir de 25 minutos a cinco el tiempo de emisión de certificados en el área de RR.HH. y de 120 a 5 en atención primaria; la revocación inmediata de los certificados de empleado público; y la trazabilidad de los emitidos.

Mayor seguridad y productividad

Según señala **Alfonso Fernández,** director de Desarrollo de Negocio en SIA, "*la colaboración que mantenemos con el Servicio de Salud de las Islas Baleares desde hace años en esta y otras iniciativas nos ha ayudado a entender sus necesidades de forma más efectiva para*.

poder facilitarle así la solución más adecuada. Los resultados alcanzados avalan una vez más la idoneidad de la propuesta tecnológica de SIA".

El proyecto, que ha alcanzado la tramitación de **500 solicitudes de permisos y 3.000 solicitudes de certificado centralizado** desde octubre de 2018, dota al profesional de una única credencial/contraseña, de acceso inmediato a los sistemas desde la contratación, implanta sistemas de recuperación rápida de contraseñas, incorpora al ciclo de vida de la identidad la gestión del certificado electrónico centralizado y da respuesta a los requerimientos legales.

El resultado final es un sistema que incrementa la seguridad y la productividad, a la vez que disminuye costes y el esfuerzo redundante en aras del ciudadano, un paso más hacia delante de la Administración Pública balear en la modernización de la prestación del servicio sanitario a través de las Tecnologías de la Información.

El servicio de Salud de Baleares garantiza con SIA la seguridad en el acceso a sus sistemas de Información

A través de esta iniciativa, desarrollada por SIA, el Servicio de Salud de las Islas Baleares ha logrado optimizar el día a día de sus más de 18.000 profesionales y mejorar el servicio a los ciudadanos, alcanzando altos niveles de eficiencia y eficacia en términos de seguridad, tiempo, costes y cumplimiento legal

El **Servicio de Salud de las Islas Baleares (IB-Salut)** ha depositado su confianza, una vez más, en SIA (Sistemas Informáticos Abiertos), proveedor líder de seguridad y servicios de administración de TI, para abordar la evolución de su sistema de Gestión de Identidades (GID) a través de la actualización de la versión desplegada, dotando a la plataforma del soporte profesional necesario y de nuevas funcionalidades.

El sistema de **Gestión de Identidade**s de que dispone el organismo balear aborda la gestión de la identificación y el control de acceso de sus profesionales a la información y se implementó en torno a un modelo de roles y responsabilidades que unifica el acceso a los Sistemas de Información de atención primaria (159 centros de salud) y de atención especializada (diez hospitales) y un autoservicio de provisión de identidades para facilitar la movilidad entre los centros.

Mejor comunicación con los usuarios

Este sistema permite que el personal de IB-Salut se encuentre **localizado organizativamente** de modo adecuado y los permisos que se le atribuyen tengan una correspondencia directa con el rol laboral que desempeñan en todo momento. "*Nuestra vocación de servicio público ha sido y es el eje central de las mejoras tecnológicas emprendidas en el IB-Salut; gracias a este proyecto, nuestros profesionales pueden disponer de acceso inmediato a los Sistemas de Información que necesitan para el ejercicio de sus funciones, desde el momento de su incorporación al organismo, lo que garantiza que los ciudadanos disfruten de una correcta y*

completa atención asistencial", apunta **Miguel Ángel Benito**, jefe del Servicio de Seguridad de la Información en IB-Salut.

Entre otras cuestiones, la actualización del sistema de GID ha logrado mejorar las comunicaciones a los usuarios, el cumplimiento normativo (RGPD y Esquena Nacional de Seguridad), la gestión de credenciales privilegiadas de administradores y ha incorporado el portal de autoservicio de GID (IBSalut-Store), a través del cual los profesionales pueden solicitar el acceso a aquellos sistemas que no se le han asignado por regla de negocio según su perfil.

Portal único

Se trata de un **único portal y procedimiento para la solicitud de permisos** que logra eliminar los desplazamientos de los profesionales, simplificar la tarea de aprobación delas solicitudes, asignar automáticamente los permisos y ofrecer la trazabilidad de las autorizaciones de permisos a acceso.Además, entre otros recursos, IBSalut-Store permite acceder al certificado electrónico centralizado, que posibilita autenticarse y. firmar documentos electrónicos desde cualquier dispositivo con acceso a internet y sin equipamiento adicional.

Con motivo de la puesta en marcha del servicio de firma centralizada en el Servicio de Salud de las Islas Baleares, también de la mano de SIA, se ha **integrado el sistema de GID con la Autoridad de Certificación de SIA.**

Esta integración, que supone la gestión de la solicitud del certificado por parte del profesional, aprobación o rechazo de la solicitud desde el área de Recursos Humanos y la revocación del certificado, ha conseguido reducir de 25 minutos a cinco el tiempo de emisión de certificados en el área de RR.HH. y de 120 a 5 en atención primaria; la revocación inmediata de los certificados de empleado público; y la trazabilidad de los emitidos.

Mayor seguridad y productividad

Según señala **Alfonso Fernández,** director de Desarrollo de Negocio en SIA, "*la colaboración que mantenemos con el Servicio de Salud de las Islas Baleares desde hace años en esta y otras iniciativas nos ha ayudado a entender sus necesidades de forma más efectiva para*

poder facilitarle así la solución más adecuada. Los resultados alcanzados avalan una vez más la idoneidad de la propuesta tecnológica de SIA".

El proyecto, que ha alcanzado la tramitación de **500 solicitudes de permisos y 3.000 solicitudes de certificado centralizado** desde octubre de 2018, dota al profesional de una única credencial/contraseña, de acceso inmediato a los sistemas desde la contratación, implanta sistemas de recuperación rápida de contraseñas, incorpora al ciclo de vida de la identidad la gestión del certificado electrónico centralizado y da respuesta a los requerimientos legales.

El resultado final es un sistema que incrementa la seguridad y la productividad, a la vez que disminuye costes y el esfuerzo redundante en aras del ciudadano, un paso más hacia delante de la Administración Pública balear en la modernización de la prestación del servicio sanitario a través de las Tecnologías de la Información.

Interempresas.net | INFORMÁTICA Y COMUNICACIONES

6 Mayo 2019

La organización ha logrado optimizar el día a día de sus más de 18.000 profesionales

El Servicio de Salud de las Islas Baleares garantiza la seguridad en el acceso a sus sistemas de Información con SIA

El Servicio de Salud de las Islas Baleares (IB-Salut) ha depositado su confianza, una vez más, en SIA (Sistemas Informáticos Abiertos), proveedor de seguridad y servicios de administración de TI, para abordar la evolución de su sistema de Gestión de Identidades (GID) a través de la actualización de la versión desplegada, dotando a la plataforma del soporte profesional necesario y de nuevas funcionalidades.

El sistema de Gestión de Identidades de que dispone el organismo balear aborda la gestión de la identificación y el control de acceso de sus profesionales a la información y se implementó en torno a un modelo de roles y responsabilidades que unifica el acceso a los Sistemas de Información de atención primaria (159 centros de salud) y de atención especializada (diez hospitales) y un autoservicio de provisión de identidades para facilitar la movilidad entre los centros.

Este sistema permite que el personal de IB-Salut se encuentre localizado organizativamente de modo adecuado y los permisos que se le atribuyen tengan una correspondencia directa con el rol laboral que desempeñan en todo momento.

“Nuestra vocación de servicio público ha sido y es el eje central de las mejoras tecnológicas emprendidas en el IB-Salut; gracias a este proyecto, nuestros profesionales pueden disponer de acceso inmediato a los Sistemas de Información que necesitan para el ejercicio de sus funciones, desde el momento de su incorporación al organismo, lo que garantiza que los ciudadanos disfruten de una correcta y completa atención asistencial”, apunta Miguel Ángel Benito, jefe del Servicio de Seguridad de la Información en IB-Salut.

Entre otras cuestiones, la actualización del sistema de GID ha logrado mejorar las comunicaciones a los usuarios, el cumplimiento normativo (RGPD y Esquema Nacional de

Seguridad), la gestión de credenciales privilegiadas de administradores y ha incorporado el portal de autoservicio de GID (IBSalut-Store), a través del cual los profesionales pueden solicitar el acceso a aquellos sistemas que no se le han asignado por regla de negocio según su perfil.

El Servicio de Salud de las Islas Baleares evoluciona su sistema de Gestión de Identidades (GID) a través de la actualización de la versión que ya tenía desplegada.

Simplificar las tareas

Se trata de un único portal y procedimiento para la solicitud de permisos que logra eliminar los desplazamientos de los profesionales, simplificar la tarea de aprobación de las solicitudes, asignar automáticamente los permisos y ofrecer la trazabilidad de las autorizaciones de permisos a acceso. Además, entre otros recursos, IBSalut-Store permite acceder al certificado electrónico centralizado, que posibilita autenticarse y firmar documentos electrónicos desde cualquier dispositivo con acceso a internet y sin equipamiento adicional.

Con motivo de la puesta en marcha del servicio de firma centralizada en el Servicio de Salud de las Islas Baleares, también de la mano de SIA, se ha integrado el sistema de GID con la Autoridad de Certificación de SIA.

Esta integración, que supone la gestión de la solicitud del certificado por parte del profesional, aprobación o rechazo de la solicitud desde el área de Recursos Humanos y la revocación del certificado, ha conseguido reducir de 25 minutos a cinco el tiempo de emisión de certificados en el área de RR.HH. y de

120 a cinco en atención primaria; la revocación inmediata de los certificados de empleado público; y la trazabilidad de los emitidos.

Los resultados avalan la propuesta

Según señala Alfonso Fernández, director de Desarrollo de Negocio en SIA, “la colaboración que mantenemos con el Servicio de Salud de las Islas Baleares desde hace años en esta y otras iniciativas nos ha ayudado a entender sus necesidades de forma más efectiva para poder facilitarle así la solución más adecuada. Los resultados alcanzados avalan una vez más la idoneidad de la propuesta tecnológica de SIA”.

El proyecto, que ha alcanzado la tramitación de 500 solicitudes de permisos y 3.000 solicitudes de certificado centralizado desde octubre de 2018, dota al profesional de una única credencial/contraseña, de acceso inmediato a los sistemas desde la contratación, implanta sistemas de recuperación rápida de contraseñas, incorpora al ciclo de vida de la identidad la gestión del certificado electrónico centralizado y da respuesta a los requerimientos legales.

El resultado final es un sistema que incrementa la seguridad y la productividad, a la vez que disminuye costes y el esfuerzo redundante en aras del ciudadano, un paso más hacia delante de la Administración Pública balear en la modernización de la prestación del servicio sanitario a través de las Tecnologías de la Información.

Expansión

7 Mayo 2019

EMPRENDEDORES

Una 'start up' española en la cima de Silicon Valley

Fundada por el madrileño Eduardo Villar, Returnly acaba de cerrar una ronda de 17 millones de euros y tiene a los fundadores de gigantes como Yammer y PayPal como padrinos. Por Javier G. Fernández

PISTAS

Carrefour usa 'blockchain' para certificar el pescado

Baleares garantiza la seguridad del servicio de salud

El Servicio de Salud de las Islas Baleares (IB-Salut) ha confiado en SIA (Sistemas Informáticos Abiertos), proveedor de servicios de seguridad y de administración de TI, para abordar la evolución de su sistema de Gestión de Identidades (GID) a través de la actualización de la versión desplegada. El sistema de Gestión de Identidades aborda la gestión de la identificación y el control de acceso de los profesionales a la información. Se implementó en torno a un modelo de roles y responsabilidades que unifica el acceso a los sistemas de información de atención primaria (159 centros de salud), sus diez hospitales y un autoservicio de provisión de identidades para facilitar la movilidad entre los centros.

elEconomista.es

16 Mayo 2019

El servicio de salud de las Islas Baleares garantiza con SIA la seguridad en el acceso a sus sistemas de información

IB-Salut ha logrado optimizar el día a día de sus más de 18.000 profesionales

El Servicio de Salud de las Islas Baleares (IB-Salut) ha depositado su confianza, una vez más, en SIA (Sistemas Informáticos Abiertos), proveedor líder de seguridad y servicios de administración de TI, para abordar la evolución de su sistema de Gestión de Identidades (GID) a través de la actualización de la versión desplegada, dotando a la plataforma del soporte profesional necesario y de nuevas funcionalidades.

El sistema de Gestión de Identidades de que dispone el organismo balear aborda la gestión de la identificación y el control de acceso de sus profesionales a la información y se implementó en torno a un modelo de roles y responsabilidades que unifica el acceso a los Sistemas de Información de atención primaria (159 centros de salud) y de atención especializada (diez hospitales) y un autoservicio de provisión de identidades para facilitar la movilidad entre los centros.

Este sistema permite que el personal de IB-Salut se encuentre localizado organizativamente de modo adecuado y los permisos que se le atribuyen tengan una correspondencia directa con el rol laboral que desempeñan en todo momento.

"Nuestra vocación de servicio público ha sido y es el eje central de las mejoras tecnológicas emprendidas en el IB-Salut; gracias

a este proyecto, nuestros profesionales pueden disponer de acceso inmediato a los Sistemas de Información que necesitan para el ejercicio de sus funciones, desde el momento de su incorporación al organismo, lo que garantiza que los ciudadanos disfruten de una correcta y completa atención asistencial", apunta Miguel Ángel Benito, jefe del Servicio de Seguridad de la Información en IB-Salut.

Entre otras cuestiones, la actualización del sistema de GID ha logrado mejorar las comunicaciones a los usuarios, el cumplimiento normativo (RGPD y Esquena Nacional de Seguridad), la gestión de credenciales privilegiadas de administradores y ha incorporado el portal de autoservicio de GID (IBSalut-Store), a través del cual los profesionales pueden solicitar el acceso a aquellos sistemas que no se le han asignado por regla de negocio según su perfil.

Se trata de un único portal y procedimiento para la solicitud de permisos que logra eliminar los desplazamientos de los profesionales, simplificar la tarea de aprobación de las solicitudes, asignar automáticamente los permisos y ofrecer la trazabilidad de las autorizaciones de permisos a acceso.

Además, entre otros recursos, IBSalut-Store permite acceder al certificado electrónico centralizado, que posibilita autenticarse y firmar documentos electrónicos desde cualquier dispositivo con acceso a Internet y sin equipamiento adicional.

Con motivo de la puesta en marcha del servicio de firma centralizada en el Servicio de Salud de las Islas Baleares, también de la mano de SIA, se ha integrado el sistema de GID con la Autoridad de Certificación de SIA.

Esta integración, que supone la gestión de la solicitud del certificado por parte del profesional, aprobación o rechazo de la solicitud desde el área de Recursos Humanos y la revocación del certificado, ha conseguido reducir de 25 minutos a cinco el tiempo de emisión de certificados en el área de RR.HH. y de 120 a 5 en atención primaria; la revocación inmediata de los certificados de empleado público; y la trazabilidad de los emitidos.

Según señala Alfonso Fernández, director de Desarrollo de Negocio en SIA, "la colaboración que mantenemos con el Servicio de Salud de las Islas Baleares desde hace años en esta y otras iniciativas nos ha ayudado a entender sus necesidades de forma más efectiva para poder facilitarle así la solución más adecuada. Los resultados alcanzados avalan una vez más la

idoneidad de la propuesta tecnológica de SIA".
El proyecto, que ha alcanzado la tramitación de 500 solicitudes de permisos y 3.000 solicitudes de certificado centralizado desde octubre de 2018, dota al profesional de una única credencial/contraseña, de acceso inmediato a los sistemas desde la contratación, implanta sistemas de recuperación rápida de contraseñas, incorpora al ciclo de vida de la identidad la gestión del certificado electrónico centralizado y da respuesta a los requerimientos legales.
El resultado final es un sistema que incrementa la seguridad y la productividad, a la vez que disminuye costes y el esfuerzo redundante en aras del ciudadano, un paso más hacia delante de la Administración Pública balear en la modernización de la prestación del servicio sanitario a través de las Tecnologías de la Información.

empresa

noticias

Prosegur presenta en España Cipher, la compañía en la que concentrará sus servicios de ciberseguridad

Prosegur acaba de materializar su transformación hacia la convergencia de seguridades con la presentación en España, el 13 de junio, de Cipher, la empresa de ciberseguridad brasileña que adquirió a finales del año pasado. Se trata de una firma de referencia no solo en Brasil, sino también en otros países como Estados Unidos.

"Hace cinco años nos enfocábamos a soluciones globales de seguridad y hoy estamos en un entorno en el que se mide lo físico y lo lógico", afirmó José Gil, director general comercial de Prosegur. Es ahí donde encajará Cipher mediante su aportación de un amplio portfolio de servicios como son la consultoría, análisis de vulnerabilidades, investigación forense, cibervigilancia, cumplimiento normativo, Red Team, respuesta gestionada, hacking ético, seguridad cloud o inteligencia, entre otros.

A través de Cipher, Prosegur podrá dar servicio en 25 países de todos los continentes. Para ello cuenta además con seis centros de operaciones de seguridad, entre los cuales uno se encuentra en Madrid. El resto se ubican en Estados Unidos, Brasil, Colombia, Portugal y Paraguay para "dar capacidad global a los clientes", apuntó Alejandro Alonso, presidente ejecutivo de Cipher.

A la presentación asistió Ed Bounds, que fundó Cipher en el año 2000 y la ha situado como una referencia. Según explicó, la compañía es capaz de analizar diariamente 1.000 millones de eventos y más de 10.000 amenazas. Cuenta además con dos millones de usuarios protegidos y 200.000 activos de seguridad gestionados. La firma desarrolla sus operaciones las 24 horas del día todos los días del año. ■

El Instituto de Técnica Aeroespacial protege toda su red con la tecnología de Fortinet

El Instituto de Técnica Aeroespacial (INTA), organismo público de investigación dependiente del Ministerio de Defensa, ha confiado en las soluciones de Fortinet para la protección de su red. El Instituto ha desplegado un conjunto de productos de seguridad que le proporcionan protección y visibilidad de cada segmento de red y dispositivo, ya sea virtual, en la nube o alojado en sus centros de datos. Con ellos, el INTA cumple también con las diferentes políticas de seguridad y puede gestionar sincronizadamente sus respuestas ante amenazas procedentes de cualquier elemento de la red. Asimismo, le suministra capacidad para monitorizar y gestionar todas las soluciones desplegadas desde una única consola, lo que redunda en menores costes de gestión y personal.

El proyecto ha contemplado el despliegue de firewalls de nueva generación que le permiten al INTA abordar nuevas funcionalidades, como descifrado de tráfico y análisis de tráfico cifrado. De igual manera, cuenta con una solución de autenticación centralizada y otra para la protección y análisis de sus aplicaciones web.

Todo esto se une a soluciones de protección del correo electrónico, para la salvaguarda del endpoint, de visibilidad de todos los eventos, de análisis de posibles amenazas desconocidas y del comportamiento del usuario, entre otras. ■

SIA actualiza el sistema de gestión de identidades del Servicio Balear de Salud

El Servicio de Salud de las Islas Baleares ha depositado su confianza, una vez más, en SIA (Sistemas Informáticos Abiertos) para abordar la evolución de su sistema de gestión de identidades a través de la actualización de la versión desplegada. La plataforma cuenta así con el soporte profesional necesario y con nuevas funcionalidades.

Entre otras cuestiones, la actualización de este sistema ha logrado mejorar las comunicaciones a los usuarios, el cumplimiento normativo y la gestión de credenciales privilegiadas de administradores. Además, permite que el personal se encuentre localizado y organizado.

X by Orange garantiza la seguridad en la nube gracias a Check Point

Las soluciones de Check Point Software Technologies han sido las elegidas para fortalecer la oferta de seguridad cloud de X by Orange, la división de tecnología B2B de Orange en España. En concreto, ha implementado los productos Check Point CloudGuard para AWS y Check Point ZoneAlarm para proporcionar a sus clientes pymes soluciones de seguridad en la nube, dispositivos móviles y puestos de trabajo.

El objetivo de X by Orange es permitir el acceso a los servicios digitales a través de la nube, ofreciendo aquellas funciones que las pymes necesitan a un precio competitivo y sin exigir a cambio un compromiso a largo plazo.

SIA actualiza el sistema de gestión de identidades del Servicio Balear de Salud

El Servicio de Salud de las Islas Baleares ha depositado su confianza, una vez más, en SIA (Sistemas Informáticos Abiertos) para abordar la evolución de su sistema de gestión de identidades a través de la actualización de la versión desplegada. La plataforma cuenta así con el soporte profesional necesario y con nuevas funcionalidades.

Entre otras cuestiones, la actualización de este sistema ha logrado mejorar las comunicaciones a los usuarios, el cumplimiento normativo y la gestión de credenciales privilegiadas de administradores. Además, permite que el personal se encuentre localizado y organizado.

El IB-Salut de Baleares agiliza el acceso a los sistemas de información sanitarios

El servicio de salud ha colaborado con SIA en la transformación de su plataforma de gestión de identidades y la integración de la firma centralizada.

La integración de las herramientas tecnológicas en los sistemas sanitarios se está abordando en España desde distintos ángulos. En Cataluña se está confiando en la nube para la gestión de las herramientas de imagen médica. En Madrid, los centros públicos han incorporado soluciones de comunicaciones para facilitar la realización de videollamadas con las que agilizar diagnósticos. El SERGAS gallego está probando la introducción de mejoras en el acceso al historial del paciente.

A estos se suma IB-Salut. El Servicio de Salud de las Islas Baleares ha actualizado su sistema de Gestión de Identidades, GID, de la mano de SIA-Sistemas Informáticos Abiertos. El proceso ha mejorado las funcionalidades del servicio, que se encarga de administrar los perfiles de los profesionales sanitarios de Baleares y de darles los accesos necesarios, vinculando los permisos al rol de cada persona y facilitando la movilidad entre los 159 centros de atención primaria y los 10 hospitales para atención especializada. Así, los especialistas tienen disponible en todo momento el acceso a la información necesaria para la asistencia a pacientes a través de una única credencial.

Esta modernización ha permitido añadir el portal de

autoservicio de GID IBSalut-Store, que permite que el personal sanitario solicite acceso a otros recursos, en los que inicialmente no se les encuadra, a través de un único portal y procedimiento. Esto evita los desplazamientos y agiliza los trámites administrativos para el solicitante, pero también garantiza la trazabilidad y el cumplimiento para los gestores, y acelera los procesos de aprobación o revocación. Con el servicio se ha implantado el certificado electrónico centralizado, con el cual los usuarios pueden autenticarse y firmar de forma digital, sin necesidad de otro recurso que el acceso a internet.

El sistema de GID se ha integrado con la Autoridad de Certificación de SIA, lo que agiliza los tiempos de emisión de certificados en el departamento de recursos humanos y de atención primaria: se ha pasado de tardar 120 minutos a 5 en este último servicio, mientras que en el área de personal, los tiempos se han recortado desde los 25 minutos de antes a los 5 de ahora.

Entre otras funcionalidades, la revisión de la plataforma ha servido para optimizar la comunicación a los usuarios del sistema, el cumplimiento normativo con la adopción de nuevas regulaciones como el GDPR o la gestión de credenciales privilegiadas de administradores.

Grupo SIA incrementa su facturación un 22% hasta los 57 millones de euros

Grupo SIA (Sistemas Informáticos Abiertos), ha dado a conocer sus resultados económicos correspondientes al ejercicio fiscal 2018 (del 1 de enero al 31 de diciembre de 2018), que ha cerrado con una facturación de 57 millones de euros y un EBITDA superior a los 5 millones.

Grupo SIA (Sistemas Informáticos Abiertos), proveedor íder de soluciones de seguridad y servicios de administración de TI, ha cerrado el ejercicio fiscal 2018 con una facturación de **57 millones de euros,** lo que supone un crecimiento del 22% con respecto al año anterior. El grupo, que opera en España y Portugal, alcanzó también un E**BITDA superior a los 5 millones de euro**s.

"Estos resultados confirman la tendencia del crecimiento de doble dígito de los ingresos y el EBITDA de los últimos años como resultado de la expansión del mercado de Ciberseguridad, la inversión en tecnología propia de Firma Digital en la nube y las iniciativas de transformación que han formado parte de nuestro plan de negocio 2014-2018", apunta **Enrique Palomares**, CEO del Grupo SIA.

Equipo profesional experimentado

La evolución de los resultados del grupo se basa fundamentalmente en la labor del equipo profesional de expertos acreditados que lo conforma, con amplia experiencia y conocimiento en cada ámbito tecnológico. Durante 2018, **la plantilla de SIA ha crecido un 14%** y, en la actualidad, cuenta con más de 700 personas entre ambas geografías.

La compañía, en este sentido, continúa su compromiso de fomentar la creación de empleo cualificado y estable y la formación de sus profesionales. Los esfuerzos se centran principalmente en identificar y desarrollar el potencial de las personas, con el fin de ofrecer oportunidades de carrera y orientar el desempeño a dar el mejor servicio a sus clientes.

En este sentido, cabe destacar, por un lado, que SIA cuenta entre sus filas con 212 personas con certificaciones, sumando un total de 534 en vigor; y, por

otro, su apuesta por la incorporación de perfiles junior con vocación STEM (disciplinas académicas de Ciencia, Tecnología, Ingeniería y Matemáticas); el año pasado, 30 jóvenes de los 34 que finalizaron sus prácticas en la compañía, eligieron continuar en SIA su carrera profesional.

Los resultados alcanzados en cada una de las **divisiones de negocio** del grupo representan un 20% en Consultoría, un 56% en Infraestructuras y Proyectos y un 24% en Cloud & Servicios Profesionales.

Por industrias, la compañía tiene presencia en todos los sectores de actividad distribuida de la siguiente manera: un 22% en Administraciones Públicas y Sanidad, un 24% en Banca y Seguros, un 14% en Industria y Servicios y un 40% en Telco y Media.

SIA en España

El mercado español sigue representando la principal fuente de crecimiento del grupo. En el ejercicio fiscal 2018 alcanzó una facturación cercana a los **48 millones de euros,** lo que significa un aumento del 22% frente al año anterior. SIA en España gestiona más de mil proyectos al año.

CESCE SI en Portugal

En el mercado portugués, Grupo SIA opera a través de la marca CESCE SI, proveedor líder en soluciones de Almacenamiento de Datos y que adquirió en 2004. CESCE cerró el ejercicio fiscal con una cifra de negocio de **9,4 millones de euro**s, lo que supone un incremento del 25% con respecto a 2017. En el país vecino, está presente en todos los sectores de actividad portugueses, principalmente en Banca, Telco y Media e Industria y Servicios.

Este año tanto SIA como CESCE SI celebran **30 años de trayectoria** en el mercado español y portugués respectivamente.

Grupo SIA incrementa su facturación un 22% hasta los 57 millones de euros

Grupo SIA (Sistemas Informáticos Abiertos), ha dado a conocer sus resultados económicos correspondientes al ejercicio fiscal 2018 (del 1 de enero al 31 de diciembre de 2018), que ha cerrado con una facturación de 57 millones de euros y un EBITDA superior a los 5 millones

Grupo SIA (Sistemas Informáticos Abiertos), proveedor íder de soluciones de seguridad y servicios de administración de TI, ha cerrado el ejercicio fiscal 2018 con una facturación de **57 millones de euros,** lo que supone un crecimiento del 22% con respecto al año anterior. El grupo, que opera en España y Portugal, alcanzó también un E**BITDA superior a los 5 millones de euro**s.

"Estos resultados confirman la tendencia del crecimiento de doble dígito de los ingresos y el EBITDA de los últimos años como resultado de la expansión del mercado de Ciberseguridad, la inversión en tecnología propia de Firma Digital en la nube y las iniciativas de transformación que han formado parte de nuestro plan de negocio 2014-2018", apunta **Enrique Palomares**, CEO del Grupo SIA.

Equipo profesional experimentado

La evolución de los resultados del grupo se basa fundamentalmente en la labor del equipo profesional de expertos acreditados que lo conforma, con amplia experiencia y conocimiento en cada ámbito tecnológico. Durante 2018, **la plantilla de SIA ha crecido un 14%** y, en la actualidad, cuenta con más de 700 personas entre ambas geografías.

La compañía, en este sentido, continúa su compromiso de fomentar la creación de empleo cualificado y estable y la formación de sus profesionales. Los esfuerzos se centran principalmente en identificar y desarrollar el potencial de las personas, con el fin de ofrecer oportunidades de carrera y orientar el desempeño a dar el mejor servicio a sus clientes.

En este sentido, cabe destacar, por un lado, que SIA cuenta entre sus filas con 212 personas con certificaciones, sumando un total de 534 en vigor; y, por

otro, su apuesta por la incorporación de perfiles junior con vocación STEM (disciplinas académicas de Ciencia, Tecnología, Ingeniería y Matemáticas); el año pasado, 30 jóvenes de los 34 que finalizaron sus prácticas en la compañía, eligieron continuar en SIA su carrera profesional.

Los resultados alcanzados en cada una de las **divisiones de negocio** del grupo representan un 20% en Consultoría, un 56% en Infraestructuras y Proyectos y un 24% en Cloud & Servicios Profesionales.

Por industrias, la compañía tiene presencia en todos los sectores de actividad distribuida de la siguiente manera: un 22% en Administraciones Públicas y Sanidad, un 24% en Banca y Seguros, un 14% en Industria y Servicios y un 40% en Telco y Media.

SIA en España

El mercado español sigue representando la principal fuente de crecimiento del grupo. En el ejercicio fiscal 2018 alcanzó una facturación cercana a los **48 millones de euros,** lo que significa un aumento del 22% frente al año anterior. SIA en España gestiona más de mil proyectos al año.

CESCE SI en Portugal

En el mercado portugués, Grupo SIA opera a través de la marca CESCE SI, proveedor líder en soluciones de Almacenamiento de Datos y que adquirió en 2004. CESCE cerró el ejercicio fiscal con una cifra de negocio de **9,4 millones de euro**s, lo que supone un incremento del 25% con respecto a 2017. En el país vecino, está presente en todos los sectores de actividad portugueses, principalmente en Banca, Telco y Media e Industria y Servicios.

Este año tanto SIA como CESCE SI celebran **30 años de trayectoria** en el mercado español y portugués respectivamente.

Desarticulado un clan familiar especializado en el robo de vehículos para su posterior venta en África

La **Guardia Civil** ha recuperado 57 vehículos robados principalmente en la provincia de Madrid cuyo destino era su venta en Marruecos. Hay ocho personas detenidas, varias de ellas pertenecientes a una misma unidad familiar, a las que también se les imputan robos con fuerza en ocho farmacias.

En los registros realizados durante la operación también se ha recuperado abundante material utilizado en la falsificación de placas de matrícula y troquelado de números de bastidor.

La investigación se inició tras el análisis de la información obtenida en distintos puertos marítimos españoles con conexión con Marruecos. En concreto, este análisis se llevó a cabo al detectarse varios vehículos con destino a dicho país de un mismo modelo con la misma numeración de placa de matrícula, pese a sus distintos colores y características.

Tras identificar a varios de los responsables de un posible hecho delictivo y una vez analizada su manera de actuar, los agentes corroboraron cómo el cabecilla del grupo criminal, que estaba perfectamente organizado, aprovechaba la infraestructura y cobertura de la que disponía en su país natal para vender allí los vehículos sustraídos.

Para más información: www.guardiacivil.es

La USC apuesta por SIA para implantar la firma cualificada en la nube

La Universidad de Santiago de Compostela (USC) ha confiado en **SIA (Sistemas Informáticos Abiertos)** para implantar un servicio en la nube de firma electrónica cualificada por parte del usuario final de los documentos generados en los sistemas de información de la organización académica que requieren su firma.

Con esta iniciativa, pionera entre las universidades gallegas, la institución dispone de un sistema de firma digital, basado en la emisión y utilización de certificados cualificados centralizados por parte de SIA, que combina la agilidad de su puesta en marcha, la facilidad de uso y todas las garantías de seguridad jurídica que aporta el Reglamento eIDAS.

Para más información: www.sia.es

Incibe lanza una nueva edición del Programa de Aceleración Internacional para 'startups' de ciberseguridad

Dentro del objetivo de promover una industria de ciberseguridad fuerte para aumentar así la confianza digital, el **Instituto Nacional de Ciberseguridad (Incibe)** ha lanzado una nueva edición del Programa de Aceleración Internacional Cybersecurity Ventures 2019.

El objetivo de esta iniciativa es incentivar el desarrollo de nuevas empresas en el ámbito de la ciberseguridad y facilitar el crecimiento de compañías de reciente creación apoyando a los emprendedores en la maduración de sus proyectos. De esta manera, el proyecto ofrece apoyo intensivo a 10 *startups* para ayudarlas a madurar sus negocios con el fin de atraer inversiones y captar clientes.

Para más información: www.incibe.es

España y Senegal refuerzan la lucha contra el terrorismo y el crimen organizado

La secretaria de Estado de Seguridad, Ana Botella, mantuvo el 10 de abril una reunión con la embajadora de Senegal en Madrid, Mariame Sy, con el objetivo de reforzar la cooperación bilateral en el ámbito de la lucha contra la inmigración irregular, el terrorismo y el crimen organizado, especialmente en el ámbito del tráfico de drogas.

En la reunión se subrayó, entre otros asuntos, la necesidad de adaptar los dispositivos de vigilancia a las contingencias de cada momento y se puso en valor la buena relación existente entre ambos países haciendo frente a desafíos comunes, así como la importancia de abordar estos retos de manera coordinada.

Para más información: www.interior.gob.es

Isidro Silos, nuevo director comercial de Risco Group en México

Risco Group ha anunciado el nombramiento de **Isidro Silos** como su nuevo director comercial en México. Este profesional atesora más de 15 años de experiencia en la gestión de redes de venta de distintos sectores, entre ellos el de seguridad electrónica, llegando a ser responsable de la red indirecta de Tyco Fire and Security España.

A partir de ahora, la principal función de Silos será posicionar el catálogo de Risco en el mercado mexicano ofreciendo soluciones integrales y creando nuevas oportunidades de negocio. Así, gestionará los distribuidores y estará en contacto con los integradores de seguridad y las centrales de monitoreo.

Tras hacerse público su nombramiento, Isidro Silos ha manifestado que "es un gran reto hacerse cargo del negocio de toda la zona de México, impulsando el potencial de este mercado e instaurando nuevas oportunidades de negocio para Risco".

www.riscogroup.es

La ciberseguridad, el sector en el que más evolucionan las amenazas, los incidentes y los esfuerzos de protección

La **Fundación ESYS** ha presentado la quinta edición del *Informe de la Seguridad en España*, que pretende recoger con carácter bienal la visión de la seguridad desde la perspectiva de la sociedad civil. En este estudio se pone de manifiesto que el sector de la Ciberseguridad es el de más rápida evolución en amenazas, incidentes y esfuerzos de protección.

El documento recopila datos y legislación referidos a la ciberseguridad; seguridad física; seguridad frente al terrorismo; seguridad del transporte por carretera, ferroviario, aéreo, marítimo y pesca; de los sectores del Petróleo, Gas, Energía Eléctrica y Energía Nuclear; y seguridad ante incendios, riesgos naturales y seguridad laboral.

www.fundacionesys.com

La USC apuesta por SIA para implantar la firma cualificada en la nube

La Universidad de Santiago de Compostela (USC) ha confiado en **SIA (Sistemas Informáticos Abiertos)** para implantar un servicio en la nube de firma electrónica cualificada por parte del usuario final de los documentos generados en los sistemas de información de la organización académica que requieren su firma.

Con esta iniciativa, pionera entre las universidades gallegas, la institución dispone de un sistema de firma digital, basado en la emisión y utilización de certificados cualificados centralizados por parte de SIA, que combina la agilidad de su puesta en marcha, la facilidad de uso y todas las garantías de seguridad jurídica que aporta el Reglamento eIDAS.

Para más información: www.sia.es

computing

11 Junio 2019

SIA y Comillas ICAI colaboran para fomentar la formación en ciberseguridad

A través de su participación en el Máster de Ciberseguridad de la institución académica.

SIA, proveedor de soluciones de seguridad y servicios de administración de TI, colaborará de forma activa en el Máster en Ciberseguridad que la Universidad Pontificia Comillas, a través de la Escuela Técnica Superior de Ingeniería (Comillas ICAI), pondrá en marcha a partir de septiembre.

El programa da respuesta a la creciente demanda de perfiles con formación y experiencia en este campo y se ha creado a demanda de SIA y las otras empresas colaboradoras -Bankia, Iberdrola, Iberia y Santalucía- cubriendo así las necesidades de formación en todos los aspectos que cada uno de los sectores a los que pertenecen encuentra más relevantes.

“Los continuos ciberataques a todos los sectores y servicios esenciales y la nueva Estrategia Nacional de Ciberseguridad de abril de 2019, no hacen más que constatar el déficit de profesionales cualificados, que se estima en 350.000 en Europa para 2022. Por ese motivo, es tan importante formar ahora a quien ha de proteger a empresas y ciudadanos en los próximos años”, asegura Javier Jarauta, director del Máster de Ciberseguridad y director de Consultoría del Grupo SIA.

Durante el acto de presentación del Máster, el CN D. Enrique Cubeiro, jefe del Estado Mayor del Mando Conjunto de Ciberdefensa, habló de la importancia de abordar la respuesta a las ciberamenazas desde múltiples aspectos más allá de los puramente técnicos, como la formación, la concienciación, la

cooperación, la obtención de un marco jurídico claro y universal, entre otros. Por su parte, Alfonso Fernández, director de Desarrollo de Negocio en el área de Seguridad en SIA, participó en la mesa de debate en la que, junto con otros responsables de este ámbito, analizaron la situación actual de la Ciberseguridad.

El Máster cuenta con la participación de profesorado propio de Comillas ICAI y de especialistas en Seguridad de todos los sectores empresariales, la administración pública y los cuerpos y fuerzas de Seguridad del Estado. Al programa, apoyado inicialmente por las empresas antes mencionadas, se sumarán próximamente otras organizaciones de nuevos sectores.

Según el director de Consultoría de SIA, “como compañía referente en el sector de la Ciberseguridad, se trata de aportar nuestro granito de arena al mercado laboral y la sociedad, de reforzar nuestra atracción de talento ante la dificultad de encontrarprofesionales en este campo y de avanzar en nuestra apuesta por la especialización de calidad que demanda el mercado”.

elEconomista.es

11 Junio 2019

SIA y Comillas ICAI colaboran para fomentar la formación en ciberseguridad

SIA, proveedor líder de soluciones de Seguridad y servicios de administración de TI, colaborará de forma activa y destacada en el Máster en Ciberseguridad que la Universidad Pontificia Comillas, a través de la Escuela Técnica Superior de Ingeniería (Comillas ICAI), pondrá en marcha a partir de septiembre.

El programa da respuesta a la creciente demanda de perfiles con formación y experiencia en este campo y se ha creado a demanda de SIA y las otras empresas colaboradoras -Bankia, Iberdrola, Iberia y Santalucía- cubriendo así las necesidades de formación en todos los aspectos que cada uno de los sectores a los que pertenecen encuentra más relevantes.

"Los continuos ciberataques a todos los sectores y servicios esenciales y la nueva Estrategia Nacional de Ciberseguridad de abril de 2019, no hacen más que constatar el déficit de profesionales cualificados, que se estima en 350.000 en Europa para 2022. Por ese motivo, es tan importante formar ahora a quien ha de proteger a empresas y ciudadanos en los próximos años", asegura Javier Jarauta, director del Máster de Ciberseguridad y director de Consultoría del Grupo SIA.

Durante el acto de presentación del Máster, el CN D. Enrique Cubeiro, Jefe del Estado Mayor del Mando Conjunto de Ciberdefensa, habló de la importancia de abordar la respuesta a las ciberamenazas desde múltiples aspectos más allá de los puramente técnicos, como la formación, la concienciación, la cooperación, la obtención de un marco jurídico claro y universal, entre otros. Por su parte, Alfonso Fernández, director de Desarrollo de Negocio en el área de Seguridad en SIA, participó en la mesa de debate en la que, junto con otros responsables de este ámbito, analizaron la situación actual de

la Ciberseguridad.
El Máster cuenta con la participación de profesorado propio de Comillas ICAI y de los mejores especialistas en Seguridad de todos los sectores empresariales, la administración pública y los cuerpos y fuerzas de Seguridad del Estado. Al programa, apoyado inicialmente por las empresas antes mencionadas, se sumarán próximamente otras organizaciones de nuevos sectores.
Según el director de Consultoría de SIA, "como compañía referente en el sector de la Ciberseguridad, se trata de aportar nuestro granito de arena al mercado laboral y la sociedad, de reforzar nuestra atracción de talento ante la dificultad de encontrar profesionales en este campo y de avanzar en nuestra apuesta por la especialización de calidad que demanda el mercado".

SIA y el ICAI fomentan la formación en ciberseguridad

SIA colaborará de forma activa y destacada en el Máster en Ciberseguridad que la Universidad Pontificia Comillas, a través de la Escuela Técnica Superior de Ingeniería, Comillas ICAI, pondrá en marcha a partir de septiembre. El programa de SIA e ICAI da respuesta a la creciente demanda de perfiles con formación y experiencia en este campo y se ha creado a demanda de SIA y las otras empresas colaboradoras -Bankia, Iberdrola, Iberia y Santalucía- cubriendo así las necesidades de formación en todos los aspectos que cada uno de los sectores a los que pertenecen encuentra más relevantes.

"Los continuos ciberataques a todos los sectores y servicios esenciales y la nueva Estrategia Nacional de Ciberseguridad de abril de 2019, no hacen más que constatar el déficit de profesionales cualificados, que se estima en 350.000 en Europa para 2022. Por ese motivo, es tan importante formar ahora a quien ha de proteger a empresas y ciudadanos en los próximos años", asegura Javier Jarauta, director del Máster de Ciberseguridad y director de Consultoría del Grupo SIA.

El programa de SIA e ICAI da respuesta a la creciente demanda de perfiles con formación y experiencia en este campo

Durante el acto de presentación del Máster, el CN D. Enrique Cubeiro, Jefe del Estado Mayor del Mando Conjunto de Ciberdefensa, habló de la importancia de abordar la respuesta a las ciberamenazas desde múltiples aspectos más allá de los puramente técnicos, como la

formación, la concienciación, la cooperación, la obtención de un marco jurídico claro y universal, entre otros. Por su parte, Alfonso Fernández, director de Desarrollo de Negocio en el área de Seguridad en SIA, participó en la mesa de debate en la que, junto con otros responsables de este ámbito, analizaron la situación actual de la Ciberseguridad.

El Máster cuenta con la participación de profesorado propio de Comillas ICAI y de los mejores especialistas en Seguridad de todos los sectores empresariales, la administración pública y los cuerpos y fuerzas de Seguridad del Estado. Al programa, apoyado inicialmente por las empresas antes mencionadas, se sumarán próximamente otras organizaciones de nuevos sectores.

Según el director de Consultoría de SIA, “como compañía referente en el sector de la Ciberseguridad, se trata de aportar nuestro granito de arena al mercado laboral y la sociedad, de reforzar nuestra atracción de talento ante la dificultad de encontrar profesionales en este campo y de avanzar en nuestra apuesta por la especialización de calidad que demanda el mercado”.

Diario Informático

11 Junio 2019

SIA y el ICAI fomentan la formación en ciberseguridad

SIA colaborará de forma activa y destacada en el Máster en Ciberseguridad que la Universidad Pontificia Comillas, a través de la Escuela Técnica Superior de Ingeniería, Comillas ICAI, pondrá en marcha a partir de septiembre. El programa de SIA e ICAI da respuesta a la creciente demanda de perfiles con formación y experiencia en este campo y se ha creado a demanda de SIA y las otras empresas colaboradoras -Bankia, Iberdrola, Iberia y Santalucía- cubriendo así las necesidades de formación en todos los aspectos que cada uno de los sectores a los que pertenecen encuentra más relevantes.

"Los continuos ciberataques a todos los sectores y servicios esenciales y la nueva Estrategia Nacional de Ciberseguridad de abril de 2019, no hacen más que constatar el déficit de profesionales cualificados, que se estima en 350.000 en Europa para 2022. Por ese motivo, es tan importante formar ahora a quien ha de proteger a empresas y ciudadanos en los próximos años", asegura Javier Jarauta, director del Máster de Ciberseguridad y director de Consultoría del Grupo SIA.

El programa de SIA e ICAI da respuesta a la creciente demanda de perfiles con formación y experiencia en este campo

Durante el acto de presentación del Máster, el CN D. Enrique Cubeiro, Jefe del Estado Mayor del Mando Conjunto de Ciberdefensa, habló de la importancia de abordar la respuesta a las ciberamenazas desde múltiples aspectos más allá de los puramente técnicos, como la

formación, la concienciación, la cooperación, la obtención de un marco jurídico claro y universal, entre otros. Por su parte, Alfonso Fernández, director de Desarrollo de Negocio en el área de Seguridad en SIA, participó en la mesa de debate en la que, junto con otros responsables de este ámbito, analizaron la situación actual de la Ciberseguridad.

El Máster cuenta con la participación de profesorado propio de Comillas ICAI y de los mejores especialistas en Seguridad de todos los sectores empresariales, la administración pública y los cuerpos y fuerzas de Seguridad del Estado. Al programa, apoyado inicialmente por las empresas antes mencionadas, se sumarán próximamente otras organizaciones de nuevos sectores.

Según el director de Consultoría de SIA, “como compañía referente en el sector de la Ciberseguridad, se trata de aportar nuestro granito de arena al mercado laboral y la sociedad, de reforzar nuestra atracción de talento ante la dificultad de encontrar profesionales en este campo y de avanzar en nuestra apuesta por la especialización de calidad que demanda el mercado”.

Expansión

12 Junio 2019

a de piratas

nidas, jefes de Estado y agencias de inteligencia de IntactPhone. **Por Mehul Srivastava (Financial Times)**

Communitake se propuso en 2012 construir un teléfono que no pudiera piratearse

La compañía está trabajando en una versión comercial que imite la apariencia de un 'smartphone'

Intactphone es empleado por Naciones Unidas y jefes de Estado.

stados Unidos superará a China en 2019 omo el mayor mercado de videojuegos

Electrolux usa el 'machine learning' en un purificador

Un purificador de Electrolux, conectado a la nube de Microsoft, establecerá patrones mediante *machine learning* para eliminar partículas ultrafinas de polvo, bacterias, alérgenos y malos olores. El Pure A9, disponible en Corea, Suiza y cuatro países nórdicos, vincula sus funciones a la nube, con lo que puede mostrar datos en tiempo real sobre la calidad del aire analizado. Con el *machine learning*, puede establecer patrones sobre los momentos en los que el hogar o la oficina están deshabitados para optimizar su funcionamiento.

Formación en ciberseguridad de SIA y Comillas ICAI

El proveedor de soluciones de Seguridad y servicios de administración de TI SIA colaborará de forma activa en el Máster en Ciberseguridad que la Universidad Pontificia Comillas, a través de la Escuela Técnica Superior de Ingeniería (Comillas ICAI), pondrá en marcha a partir del mes de septiembre. El programa da respuesta a la creciente demanda de perfiles con formación y experiencia en este campo y se ha creado a demanda de SIA y las otras empresas colaboradoras (Bankia, Iberdrola, Iberia y Santalucía).

Formación en ciberseguridad de SIA y Comillas ICAI

El proveedor de soluciones de Seguridad y servicios de administración de TI SIA colaborará de forma activa en el Máster en Ciberseguridad que la Universidad Pontificia Comillas, a través de la Escuela Técnica Superior de Ingeniería (Comillas ICAI), pondrá en marcha a partir del mes de septiembre. El programa da respuesta a la creciente demanda de perfiles con formación y experiencia en este campo y se ha creado a demanda de SIA y las otras empresas colaboradoras (Bankia, Iberdrola, Iberia y Santalucía).

Interempresas.net | INFORMÁTICA Y COMUNICACIONES

14 Junio 2019

El proveedor de servicios IT participará en el 'Máster de Ciberseguridad'

SIA y Comillas ICAI colaboran para fomentar la formación en ciberseguridad

SIA colaborará de forma activa y destacada en el 'Máster en Ciberseguridad' que la Universidad Pontificia Comillas, a través de la Escuela Técnica Superior de Ingeniería (Comillas ICAI), pondrá en marcha a partir de septiembre.

El programa da respuesta a la creciente demanda de perfiles con formación y experiencia en este campo y se ha creado a demanda de SIA y las otras empresas colaboradoras -Bankia, Iberdrola, Iberia y Santalucía- cubriendo así las necesidades de formación en todos los aspectos que cada uno de los sectores a los que pertenecen encuentra más relevantes.

"Los continuos ciberataques a todos los sectores y servicios esenciales y la nueva Estrategia Nacional de Ciberseguridad de abril de 2019, no hacen más que constatar el déficit de profesionales cualificados, que se estima en 350.000 en Europa para 2022. Por ese motivo, es tan importante formar ahora a quien ha de proteger a empresas y ciudadanos en los próximos años", asegura Javier Jarauta, director del Máster de Ciberseguridad y director de Consultoría del Grupo SIA.

Durante el acto de presentación del Máster, el CN Enrique Cubeiro, jefe del Estado Mayor del Mando Conjunto de Ciberdefensa, habló de la importancia de abordar la respuesta a las ciberamenazas desde múltiples aspectos más allá de los puramente técnicos, como la formación, la concienciación, la cooperación, la obtención de un marco jurídico claro y universal, entre otros. Por su parte, Alfonso Fernández, director de Desarrollo de Negocio en el área de Seguridad en SIA, participó en la mesa de debate en la que, junto con otros responsables de este ámbito, analizaron la situación actual de la Ciberseguridad.

El Máster cuenta con la participación de profesorado propio de Comillas ICAI y de los mejores especialistas en Seguridad de todos los sectores empresariales, la administración pública y los cuerpos y fuerzas de Seguridad del Estado. Al programa, apoyado inicialmente

por las empresas antes mencionadas, se sumarán próximamente otras organizaciones de nuevos sectores. Según el director de Consultoría de SIA, “como compañía referente en el sector de la Ciberseguridad, se trata de aportar nuestro granito de arena al mercado laboral y la sociedad, de reforzar nuestra atracción de talento ante la dificultad de encontrar profesionales en este campo y de avanzar en nuestra apuesta por la especialización de calidad que demanda el mercado”.

diarioabierto.es
Información económica desde una perspectiva plural

14 Junio 2019

La española SIA colaborará en el Máster en Ciberseguridad de la Universidad de Comillas

En septiembre, en la **Escuela Técnica Superior de Ingeniería (Comillas ICAI)**, se impartirá el **Máster de Ciberseguridad**, un postgrado que responde a las necesidades reales de las empresas de diferentes sectores, para las que cada vez más la seguridad constituye de los pilares fundamentales del negocio. De hecho, uno de las perfiles más demandados en España es el de CISO (chief information security officer o máximo responsable de seguridad de la información), según se recogía en el VII estudio **Top 24 Profesiones Digitales 2019**, elaborado por Inesdi Digital Business School.

En el Máster de Ciberseguridad de Comillas ICAI, la empresa española **SIA**, proveedor de soluciones de seguridad y servicios de administración de TI, colaborará de forma activa y destacada. Este programa formativo se ha creado a demanda de SIA y de otras empresas colaboradoras —Bankia, Iberdrola, Iberia y Santalucía—, cubriendo así las necesidades de formación en todos los aspectos que cada uno de los sectores a los que pertenecen encuentra más relevantes.

En palabras de asegura **Javier Jarauta**, director del Máster de Ciberseguridad y director de Consultoría del Grupo SIA: “Los continuos ciberataques a todos los sectores y servicios esenciales y la nueva **Estrategia Nacional de Ciberseguridad de abril de 2019**, no hacen más que constatar el déficit de profesionales cualificados, que se estima en 350.000 en Europa para 2022. Por ese motivo, es tan importante formar ahora a quien ha de proteger a empresas y ciudadanos en los próximos años”,

El máster cuenta con la participación de profesorado propio de Comillas ICAI y de los mejores especialistas en seguridad de todos los sectores empresariales, la administración pública y los cuerpos y fuerzas de seguridad del Estado. Al programa, apoyado inicialmente por las empresas antes mencionadas, se sumarán próximamente otras organizaciones de nuevos

sectores.

Según el director de Consultoría de SIA, “como compañía referente en el sector de la Ciberseguridad, se trata de aportar nuestro granito de arena al mercado laboral y la sociedad, de reforzar nuestra atracción de talento ante la dificultad de encontrar profesionales en este campo y de avanzar en nuestra apuesta por la especialización de calidad que demanda el mercado”.

DATACENTERMARKET

13 Junio 2019

SIA y Comillas ICAI colaboran para fomentar la formación en ciberseguridad

A través de su participación en el Máster de Ciberseguridad de la institución académica

SIA, proveedor de soluciones de seguridad y servicios de administración de TI, colaborará de forma activa en el Máster en Ciberseguridad que la Universidad Pontificia Comillas, a través de la Escuela Técnica Superior de Ingeniería (Comillas ICAI), pondrá en marcha a partir de septiembre.

SIA, proveedor de soluciones de seguridad y servicios de administración de TI, colaborará de forma activa en el Máster en Ciberseguridad que la Universidad Pontificia Comillas, a través de la Escuela Técnica Superior de Ingeniería (Comillas ICAI), pondrá en marcha a partir de septiembre.

El programa da respuesta a la creciente demanda de perfiles con formación y experiencia en este campo y se ha creado a demanda de SIA y las otras empresas colaboradoras -Bankia, Iberdrola, Iberia y Santalucía- cubriendo así las necesidades de formación en todos los aspectos que cada uno de los sectores a los que pertenecen encuentra más relevantes.

“Los continuos ciberataques a todos los sectores y servicios esenciales y la nueva Estrategia Nacional de Ciberseguridad de abril de 2019, no hacen más que constatar el déficit de profesionales cualificados, que se estima en 350.000 en Europa para 2022. Por ese motivo, es tan importante formar ahora a quien ha de proteger a empresas y ciudadanos en los próximos años”, asegura Javier Jarauta, director del Máster de Ciberseguridad y director de Consultoría del Grupo SIA.

Durante el acto de presentación del Máster, el CN D. Enrique Cubeiro, jefe del Estado Mayor del Mando Conjunto de Ciberdefensa, habló de la importancia de abordar la respuesta a las ciberamenazas desde múltiples aspectos más allá de los puramente técnicos, como la formación, la concienciación, la cooperación, la obtención de un marco jurídico claro y universal, entre otros. Por su parte, Alfonso Fernández, director de Desarrollo de Negocio en el área de Seguridad en SIA, participó en la mesa de debate en la que, junto con otros responsables de este ámbito, analizaron la situación actual de la Ciberseguridad.

El Máster cuenta con la participación de profesorado propio de Comillas ICAI y de especialistas en Seguridad de todos los sectores empresariales, la administración pública y los cuerpos y fuerzas de Seguridad del Estado. Al programa, apoyado inicialmente por las empresas antes mencionadas, se sumarán próximamente otras organizaciones de nuevos sectores.

Según el director de Consultoría de SIA, “como compañía referente en el sector de la Ciberseguridad, se trata de aportar nuestro granito de arena al mercado laboral y la sociedad, de reforzar nuestra atracción de talento ante la dificultad de encontrar profesionales en este campo y de avanzar en nuestra apuesta por la especialización de calidad que demanda el mercado”.

SIA y Comillas ICAI colaboran para fomentar la formación en ciberseguridad

El programa da respuesta a la creciente demanda de perfiles con formación y experiencia en este campo y se ha creado a demanda de SIA y las otras empresas colaboradoras: Bankia, Iberdrola, Iberia y Santalucía

SIA, proveedor líder de soluciones de Seguridad y servicios de administración de TI, colaborará de forma activa y destacada en el Máster en Ciberseguridad que la Universidad Pontificia Comillas, a través de la Escuela Técnica Superior de Ingeniería (Comillas ICAI), pondrá en marcha a partir de septiembre.

SIA, proveedor líder de soluciones de Seguridad y servicios de administración de TI, colaborará de forma activa y destacada en el Máster en Ciberseguridad que la **Universidad Pontificia Comillas**, a través de la Escuela Técnica Superior de Ingeniería (Comillas ICAI), pondrá en marcha a partir de septiembre.

El programa da respuesta a la creciente demanda de perfiles con formación y experiencia en este campo y se ha creado a demanda de SIA y las otras empresas colaboradoras -Bankia, Iberdrola, Iberia y Santalucía- cubriendo así las necesidades de formación en todos los aspectos que cada uno de los sectores a los que pertenecen encuentra más relevantes.

“Los continuos ciberataques a todos los sectores y servicios esenciales y la nueva **Estrategia Nacional de Ciberseguridad** de abril de 2019, no hacen más que constatar el déficit de profesionales cualificados, que se estima en 350.000 en Europa para 2022. Por ese motivo, es tan importante formar ahora a quien ha de proteger a empresas y ciudadanos en los próximos años”, asegura Javier Jarauta, director del Máster de Ciberseguridad y director de Consultoría del Grupo SIA.

Durante el acto de presentación del Máster, el **CN D. Enrique Cubeiro**, Jefe del Estado Mayor del Mando Conjunto de Ciberdefensa, habló de la importancia de abordar la respuesta a las ciberamenazas desde múltiples aspectos más allá de los puramente técnicos, como la formación, la concienciación, la cooperación, la obtención

de un marco jurídico claro y universal, entre otros. Por su parte, Alfonso Fernández, director de Desarrollo de Negocio en el área de Seguridad en SIA, participó en la mesa de debate en la que, junto con otros responsables de este ámbito, analizaron la situación actual de la Ciberseguridad.

El Máster cuenta con la participación de profesorado propio de Comillas ICAI y de los mejores especialistas en Seguridad de todos los sectores empresariales, la administración pública y los cuerpos y fuerzas de Seguridad del Estado. Al programa, apoyado inicialmente por las empresas antes mencionadas, se sumarán próximamente otras organizaciones de nuevos sectores.

Según el director de Consultoría de SIA, “como compañía referente en el sector de la Ciberseguridad, se trata de aportar nuestro granito de arena al mercado laboral y la sociedad, de reforzar nuestra atracción de talento ante la dificultad de encontrar profesionales en este campo y de avanzar en nuestra apuesta por la especialización de calidad que demanda el mercado”.

CSO ESPAÑA
COMPUTERWORLD FROM IDG

SIA y la Universidad de Comillas se unen para fomentar talento en ciberseguridad

Se estima que para 2022 habrá un déficit de 350.000 personales cualificados en el sector.

La compañía **SIA y la Universidad Pontificia de Comillas** han firmado un acuerdo de colaboración para fomentar la formación en ciberseguridad mediante el **Máster de Ciberseguridad** de la propia Universidad y que se pondrá en marcha a partir de septiembre. En este programa también colaboran otras entidades privadas como **Bankia, Iberdrola, Iberia y Santalucía.**

Para Javier Jarauta, "los continuos ciberataques a todos los sectores y servicios esenciales y la nueva Estrategia Nacional de Ciberseguridad de abril de 2019, no hacen más que constatar el déficit de profesionales cualificados, que se estima en **350.000 en Europa para 2022.** Por ese motivo, es tan importante formar ahora a quien ha de proteger a empresas y ciudadanos en los próximos años".

El Máster contará con especialistas de sectores como el privado, la **Administración Pública y los cuerpos y fuerzas de Seguridad del Estado**. "Aportamos nuestro granito de arena al mercado laboral y la sociedad para reforzar nuestra atracción de talento ante la dificultad de encontrar profesionales en este campo y de avanzar en nuestra apuesta por la especialización de calidad que demanda el mercado", asegura Jarauta.

SIA
Consejero Delegado:
Enrique Palomares del Amo
Dir. Técnico: José Luis Reyes
Dirección: Avda. Europa, 2.
Alcorcón 28922 Madrid
Teléfono: 913077997
Web: sia.es
Empleados: 700
Fact. 2018: 57 mill. de euros

elEconomista.es

28 Junio 2019

Imdea impulsa con SIA el desarrollo de investigación en red

Imdea Software, la Fundación Instituto Madrileño de Estudios Avanzados en las Tecnologías de Desarrollo de Software, ha puesto en marcha junto a SIA (Sistemas Informáticos Abiertos), integrador de referencia en proyectos de interconexiones ópticas y proveedor líder de seguridad y servicios de administración de TI, un sistema de monitorización activa de todos sus enlaces de fibra óptica mediante la incorporación a su red de la tecnología denominada ADVA ALM, del proveedor de equipamiento óptico ADVA Optical Networking.

El proyecto proporciona equipamiento para monitorizar la fibra oscura de REDIMadrid, una infraestructura de comunicaciones avanzada, gestionada y desarrollada por Imdea Software, que permite el intercambio de datos a alta velocidad entre las instituciones con actividad investigadora en el ámbito de la Comunidad de Madrid y que, a su vez, proporciona tránsito hacia otras redes de investigación nacionales e internacionales a través de RedIRIS.

La infraestructura básica de transmisión de que dispone el organismo madrileño para permitir estas comunicaciones cuenta con tecnología DWDM por sus prestaciones, flexibilidad y capacidad de crecimiento y debe proveer una elevada fiabilidad, permitiendo la correcta operación de la red ante fallos derivados de cortes de tráfico. Ante estas necesidades, se hacía necesario implementar en la red mecanismos que pudiesen aumentar la calidad y disponibilidad de la infraestructura, algo que la iniciativa desarrollada con SIA logra.

Gracias a la realización de este proyecto, REDIMadrid puede

fibra óptica sobre la que se transportan los servicios, reportando información en tiempo real sobre la calidad e integridad de la misma, permitiendo una rápida detección de incidencias y, a la vez, minimizar los tiempos de reparación optimizando el potencial de sus activos de fibra y ofreciendo así servicios más sólidos y eficientes.

Según César Sánchez, director del proyecto REDIMadrid de Imdea Software, "el éxito del proyecto radica en la plena compatibilidad de la solución implantada con las soluciones de transmisión que actualmente tiene implementada IMDEA Software, por las características completamente diferenciales del equipamiento ADVA ALM y por la calidad de los servicios ofrecidos por el equipo de SIA".

Por su parte, Alejandro Díez, director de Desarrollo de Negocio en SIA, destaca que "desde nuestra posición de liderazgo en la realización de proyectos de interconexiones ópticas, hemos aportado un equipo de ingenieros propio con amplia experiencia que cuenta en su haber con multitud de proyectos de éxito implementados en los últimos 20 años". Y añade, "SIA además acompañará a la Fundación durante los próximos años con el mantenimiento de la solución".

Entre los beneficios que Imdea ha obtenido con este sistema de monitorización, se encuentran:

- Mejora la calidad de los servicios ofrecidos por REDIMadrid a los centros de investigación, mediante información en tiempo real sobre la integridad y calidad de la fibra.
- Aumenta la disponibilidad de los servicios prestados por REDIMadrid, detectando inmediatamente degradaciones e iniciando contramedidas antes de que estos servicios se vean afectados.
- Monitoriza de forma activa pero no de forma intrusiva los sistemas.
- Simplifica la operación de la red de fibra y genera gráficas OTDR.
- Gestiona la red de modo intuitivo con posibilidad de integración en sistemas de información (GIS) de forma rápida y sencilla.

Gracias al despliegue de este proyecto, realizado en un tiempo récord, Imdea Software aumentará la disponibilidad y mejorará la seguridad de la red ofreciendo servicios con mayores garantías a las instituciones con actividad investigadora adheridas a su red en el ámbito de la Comunidad de Madrid.

Además ayudará a potenciar posibilidades de comunicación sin precedentes a los investigadores en todos sus campos de actividad, desde el acceso a gran velocidad a bases de datos científicas multimedia a la transferencia masiva de información en aplicaciones de computación distribuida o el uso compartido de equipamiento de investigación.

R&T REDES&TELECOM

28 Junio 2019

Imdea Software y SIA implementan un sistema de monitorización de fibra oscura en REDIMadrid

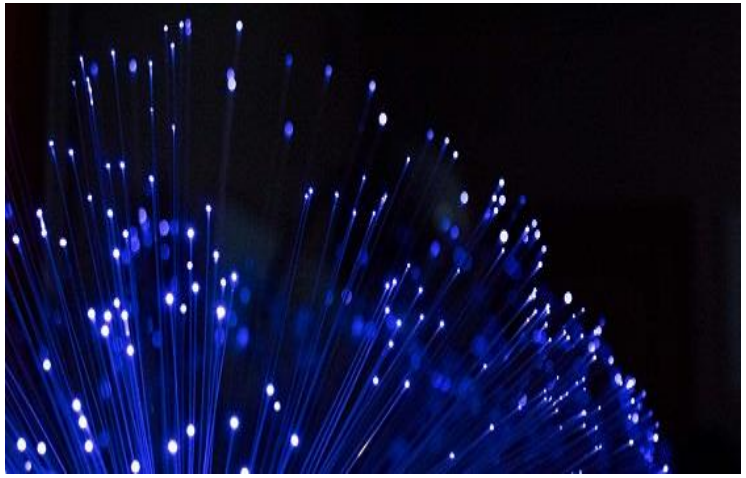
El proyecto proporciona a una de las redes de investigación regionales más avanzadas de Europa, un servicio que les permite obtener máxima funcionalidad, escalabilidad, disponibilidad y prestaciones de su infraestructura.

Imdea Software, la Fundación Instituto Madrileño de Estudios Avanzados en las Tecnologías de Desarrollo de Software, ha puesto en marcha junto a SIA(Sistemas Informáticos Abiertos), integrador de referencia en proyectos de interconexiones ópticas y proveedor de seguridad y servicios de administración de TI, un **sistema de monitorización activa de todos sus enlaces de fibra óptica** mediante la incorporación a su red de la tecnología denominada ADVA ALM, del proveedor de equipamiento óptico **ADVA Optical Networking.**

El proyecto proporciona equipamiento para monitorizar la fibra oscura de REDIMadrid, una infraestructura de comunicaciones avanzada, gestionada y desarrollada por Imdea Software, que permite el intercambio de datos a alta velocidad entre las instituciones con actividad investigadora en el ámbito de la Comunidad de Madrid y que, a su vez, proporciona tránsito hacia otras redes de investigación nacionales e internacionales a través de RedIRIS.

La infraestructura básica de transmisión de que dispone el organismo madrileño para permitir estas comunicaciones cuenta con **tecnología DWDM** por sus prestaciones, flexibilidad y capacidad de crecimiento y debe proveer una elevada fiabilidad, permitiendo la correcta operación de la red ante fallos derivados de cortes de tráfico. Ante estas necesidades, se hacía necesario implementar en la red mecanismos que pudiesen aumentar la calidad y disponibilidad de la infraestructura, algo que la iniciativa desarrollada con SIA logra.

Gracias a la realización de este proyecto, REDIMadrid puede **conocer en todo momento el estado de su infraestructura de fibra óptica sobre la que se transportan los servicios**, reportando información en tiempo real sobre la calidad e



Imdea Software y SIA implementan un sistema de monitorización de fibra oscura en REDIMadrid

integridad de la misma, permitiendo una rápida detección de incidencias y, a la vez, minimizar los tiempos de reparación optimizando el potencial de sus activos de fibra y ofreciendo así servicios más sólidos y eficientes.

Según **César Sánchez, director del proyecto REDIMadrid de Imdea Software**, "el éxito del proyecto radica en la plena compatibilidad de la solución implantada con las soluciones de transmisión que actualmente tiene implementada IMDEA Software, por las características completamente diferenciales del equipamiento ADVA ALM y por la calidad de los servicios ofrecidos por el equipo de SIA".

Por su parte, **Alejandro Díez, director de Desarrollo de Negocio en SIA**, destaca que "desde nuestra posición de liderazgo en la realización de proyectos de interconexiones ópticas, hemos aportado un equipo de ingenieros propio con amplia experiencia que cuenta en su haber con multitud de proyectos de éxito implementados en los últimos 20 años". Y añade, "SIA además acompañará a la Fundación durante los próximos años con el mantenimiento de la solución".

Entre los beneficios que Imdea ha obtenido con este sistema de monitorización, se encuentran:

-**Mejora la calidad de los servicios** ofrecidos por REDIMadrid a los centros de investigación, mediante información en tiempo real sobre la integridad y calidad de la fibra.

-**Aumenta la disponibilidad de los servicios** prestados por REDIMadrid, detectando inmediatamente degradaciones e iniciando contramedidas antes de que estos servicios se vean afectados.

-**Monitoriza de forma activa pero no de forma intrusiva los**

sistemas.

-**Simplifica la operación de la red de fibra y genera gráficas OTDR.**

-Gestiona la red de modo intuitivo con posibilidad de integración en sistemas de información (GIS) de forma rápida y sencilla.

Gracias al despliegue de este proyecto, realizado en un tiempo récord, Imdea Software aumentará la disponibilidad y mejorará la seguridad de la red ofreciendo servicios con mayores garantías a las instituciones con actividad investigadora adheridas a su red en el ámbito de la Comunidad de Madrid. Además, ayudará a potenciar posibilidades de comunicación sin precedentes a los investigadores en todos sus campos de actividad, desde el acceso a gran velocidad a bases de datos científicas multimedia a la transferencia masiva de información en aplicaciones de computación distribuida o el uso compartido de equipamiento de investigación.

computing

1 Julio 2019

IMDEA Software impulsa el desarrollo de la investigación en red

El proyecto, desarrollado con SIA, proporciona a la red de investigación regional un servicio orientado a obtener la máxima funcionalidad, escalabilidad, disponibilidad y prestaciones de la red.

Edificio del Instituto IMDEA Software

IMDEA Software, la Fundación Instituto Madrileño de Estudios Avanzados en las Tecnologías de Desarrollo de Software, ha puesto en marcha junto a SIA (Sistemas Informáticos Abiertos) un **sistema de monitorización activa de todos sus enlaces de fibra óptica** mediante la incorporación a su red de la tecnología denominada ADVA ALM, del proveedor de equipamiento óptico ADVA Optical Networking.

El proyecto proporciona equipamiento para monitorizar la fibra oscura de REDIMadrid, una infraestructura de comunicaciones, gestionada y desarrollada por Imdea Software, que permite el intercambio de datos a alta velocidad entre las instituciones con actividad investigadora en el ámbito de la Comunidad de Madrid y que, a su vez, proporciona tránsito hacia otras redes de investigación nacionales e internacionales a través de RedIRIS.

SIA monitoriza la fibra de REDIMadrid, que permite el intercambio de datos entre las instituciones investigadoras de la Comunidad de Madrid

La infraestructura básica de transmisión de que dispone el

> SIA monitoriza la fibra de REDIMadrid, que permite el intercambio de datos entre las instituciones investigadoras de la Comunidad de Madrid

organismo madrileño para permitir estas comunicaciones cuenta con tecnología DWDM y debe proveer una elevada fiabilidad, permitiendo la correcta operación de la red ante fallos derivados de cortes de tráfico. Ante estas necesidades, **se hacía necesario implementar en la red mecanismos que pudiesen aumentar la calidad y disponibilidad de la infraestructura.**

Gracias a la realización de este proyecto**, REDIMadrid puede conocer en todo momento el estado de su infraestructura de fibra óptica sobre la que se transportan los servicios**, reportando información en tiempo real sobre la calidad e integridad de esta, permitiendo una rápida detección de incidencias y, a la vez, minimizar los tiempos de reparación optimizando el potencial de sus activos de fibra y ofreciendo así servicios más sólidos y eficientes.

Según **César Sánchez, director del proyecto REDIMadrid de IMDEA Software**, "el éxito del proyecto radica en la plena compatibilidad de la solución implantada con las soluciones de transmisión que actualmente tiene implementada IMDEA Software, por las características completamente diferenciales del equipamiento ADVA ALM y por la calidad de los servicios ofrecidos por el equipo de SIA".

Beneficios

Entre los beneficios que Imdea ha obtenido con este sistema de monitorización, se encuentran:

- Mejora la calidad de los servicios ofrecidos por REDIMadrid a los centros de investigación, mediante información en tiempo real sobre la integridad y calidad de la fibra.
- Aumenta la disponibilidad de los servicios prestados por REDIMadrid, detectando inmediatamente degradaciones e iniciando contramedidas antes de que estos servicios se vean afectados.
- Monitoriza de forma activa pero no de forma intrusiva los sistemas.

- Simplifica la operación de la red de fibra y genera gráficas OTDR.
- Gestiona la red de modo intuitivo con posibilidad de integración en sistemas de información (GIS) de forma rápida y sencilla.

Gracias al despliegue de este proyecto, realizado en un tiempo récord, **IMDEA Software aumentará la disponibilidad y mejorará la seguridad de la red** ofreciendo servicios con mayores garantías a las instituciones con actividad investigadora adheridas a su red en el ámbito de la Comunidad de Madrid. Además, **ayudará a potenciar posibilidades de comunicación sin precedentes a los investigadores en todos sus campos de actividad**, desde el acceso a gran velocidad a bases de datos científicas multimedia a la transferencia masiva de información en aplicaciones de computación distribuida o el uso compartido de equipamiento de investigación.

Por su parte, Alejandro Díez, director de Desarrollo de Negocio en SIA, destaca que "desde nuestra posición de liderazgo en la realización de proyectos de interconexiones ópticas, **hemos aportado un equipo de ingenieros propio con amplia experiencia** que cuenta en su haber con multitud de proyectos de éxito implementados en los últimos 20 años". Y añade, **"SIA además acompañará a la Fundación durante los próximos años con el mantenimiento de la solución".**

Imdea impulsa con SIA un sistema de monitorización activa de todos sus enlaces de fibra óptica mediante la incorporación a su red de la tecnología ADVA ALM

El proyecto proporciona a una de las redes de investigación regionales más avanzadas un servicio orientado a obtener la máxima funcionalidad, escalabilidad, disponibilidad y prestaciones de la red

Imdea Software, la Fundación Instituto Madrileño de Estudios Avanzados en las Tecnologías de Desarrollo de Software, ha puesto en marcha junto a SIA (Sistemas Informáticos Abiertos), integrador de referencia en proyectos de interconexiones ópticas y proveedor líder de seguridad y servicios de administración de TI, un sistema de monitorización activa de todos sus enlaces de fibra óptica mediante la incorporación a su red de la tecnología denominada ADVA ALM, del proveedor de equipamiento. óptico ADVA Optical Networking.

El proyecto proporciona equipamiento para monitorizar la fibra oscura de **REDIMadrid**, una infraestructura de comunicaciones avanzada, gestionada y desarrollada por **Imdea Software**, que permite el intercambio de datos a alta velocidad entre las instituciones con actividad investigadora en el ámbito de la Comunidad de Madrid y que, a su vez, proporciona tránsito hacia otras redes de investigación nacionales e internacionales a través de **RedIRIS**.

La infraestructura básica de transmisión de que dispone el organismo madrileño para permitir estas comunicaciones cuenta con tecnología DWDM por sus prestaciones, flexibilidad y capacidad de crecimiento y debe proveer una elevada fiabilidad, permitiendo la correcta operación de la red ante fallos derivados de cortes de tráfico.

Ante estas necesidades, se hacía necesario implementar en la red mecanismos que pudiesen aumentar la calidad y disponibilidad de la infraestructura, algo que la iniciativa desarrollada con SIA logra.

Gracias a la realización de este proyecto, REDIMadrid puede conocer en todo momento el estado de su infraestructura de fibra óptica sobre la que se transportan los servicios, reportando información en tiempo real sobre la calidad e integridad de la misma, permitiendo una rápida detección de incidencias y, a la vez, minimizar los tiempos de reparación optimizando el potencial de sus activos de fibra y ofreciendo así servicios más sólidos y eficientes.

Según **César Sánchez**, director del proyecto REDIMadrid de Imdea Software, "el éxito del proyecto radica en la plena compatibilidad de la solución implantada con las soluciones de transmisión que actualmente tiene implementada IMDEA Software, por las características completamente diferenciales del equipamiento ADVA ALM y por la calidad de los servicios ofrecidos por el equipo de SIA".

Por su parte, **Alejandro Díez**, director de Desarrollo de Negocio en SIA, destaca que

"desde nuestra posición de liderazgo en la realización de proyectos de interconexiones ópticas, hemos aportado un equipo de ingenieros propio con amplia experiencia que cuenta en su haber con multitud de proyectos de éxito implementados en los últimos 20 años". Y añade, "SIA además acompañará a la Fundación durante los próximos añoscon el mantenimiento de la solución".

Entre los **beneficios** que Imdea ha obtenido con este sistema de monitorización, se encuentran:

- Mejora la calidad de los servicios ofrecidos por REDIMadrid a los centros de investigación, mediante información en tiempo real sobre la integridad y calidad de la fibra.
- Aumenta la disponibilidad de los servicios prestados por REDIMadrid, detectando inmediatamente degradaciones e iniciando contramedidas antes de que estos servicios se vean afectados.
- Monitoriza de forma activa pero no de forma intrusiva los sistemas.
- Simplifica la operación de la red de fibra y genera gráficas OTDR.
- Gestiona la red de modo intuitivo con posibilidad de integración en sistemasde información (GIS) de forma

rápida y sencilla.
Gracias al despliegue de este proyecto, realizado en un tiempo récord, Imdea Software aumentará la disponibilidad y mejorará la seguridad de la red ofreciendo servicios con mayores garantías a las instituciones con actividad investigadora adheridas a su red en el ámbito de la Comunidad de Madrid. Además ayudará a potenciar posibilidades de comunicación sin precedentes a los investigadores en todos sus campos de actividad, desde el acceso a gran velocidad a bases de datos científicas multimedia a la transferencia masiva de información en aplicaciones de computación distribuida o el uso compartido de equipamiento de investigación.

La ciberseguridad y la posición relevante de la IA

Los ataques a los sistemas informáticos de una entidad u organización son cada vez más frecuentes, tal y como estamos viendo. Acabamos de conocer impactos de diferente gravedad como el robo de información confidencial en una empresa energética o incluso el robo de millones de datos fiscales de ciudadanos y empresas de Bulgaria. Aunque existen diferentes tipologías y escalas de ataques, gran parte de ellos se diseñan para robar credenciales de acceso o para explotar brechas de seguridad filtrando datos o solicitando rescates. Casi nada se conoce de los impactos a pequeñas empresas o incluso a los particulares en este tipo de ataques.

En este "juego" de ataque-defensa desconocemos muchas variables que nos ayudarían a minimizar los impactos: cuándo se realizará su ataque, qué y cómo se pretende atacar; y fundamentalmente, cuál es la intención final del ataque. Si además añadimos que se tarda más de dos meses en descubrirse las brechas de seguridad y que se necesitan otros 50 días para contener e investigar, el escenario es totalmente negativo.

Todo lo anterior se resume en una simple frase a asumir cuanto antes: "Siempre vamos por detrás de los malos".

Sin embargo, hay una variable de la que sí podemos tomar el

control en esa situación de desventaja clara: “El tiempo entre que se sufre un ataque y se detecta en la entidad”. Esa es la variable que puede minimizarse con la Inteligencia Artificial.

Escenarios de protección. ¿Algo nuevo?

En la actualidad se desean proteger dos escenarios distintos:

- **Los sistemas de información internos en la organización:** infraestructuras, servicios, activos digitales, etc.; los cuales dependen directamente de la entidad y que pueden estar on-premise o en la nube.
- **La imagen y la reputación externa**, que depende de la percepción que tienen terceros de la propia entidad.

No es algo nuevo que haya surgido recientemente. A modo de símil, Felipe II en su basto imperio tuvo que contener amenazas internas (intrigas palaciegas, revuelta en Flandes, rebelión de los moriscos, …) y amenazas externas (la leyenda negra del Rey, batalla de Lepanto, …). En aquel momento se tenía un sistema polisinodial (conjunto de Consejos que trataban los asuntos de cada territorio/estado), que trasladaba los asuntos al Rey para la toma de decisiones. También tenían a su disposición una extensa red de espionaje para tener control de la información de lo que sucedía fuera del reino con respecto a los intereses del imperio.

La monitorización interna de los sistemas informáticos de una entidad (sensores, concentradores de logs, SIEMs, …) y la monitorización externa de redes públicas/sociales /darknet son los equivalentes a día de hoy de lo que hace cinco siglos se hacía.

La IA como extractor de patrones de comportamiento

El modelo tradicional de detección de alertas se basa en el establecimiento cuasi-manual de reglas en los sistemas de monitorización por parte de los expertos analistas. Sin embargo, dichas reglas no cubren todos los casos posibles y

suelen cambiar con una frecuencia mayor que la disponibilidad de los expertos para su actualización.

Con los volúmenes de datos almacenados de sistemas tipo firewall, IDS/IPS, antivirus, correos electrónicos, comunicaciones VPN, … y las noticias reputacionales monitorizadas (redes sociales principalmente), las alertas se van acumulando, siendo la mayoría de las veces falsos positivos. Esto ralentiza la contención de aquellas alertas que sí son maliciosas y que deben ser analizadas y contenidas cuanto antes.

La IA actúa de una manera totalmente diferente. En base al histórico de actuaciones (datos y respuestas dadas en un momento determinado) y la correlación entre sistemas con el concepto de sesión de trabajo, se puede averiguar qué reglas son las que se cumplen para esos datos. La aplicación posteriormente de dichas reglas en los sistemas tradicionales de monitorización y alerta permite tener sistemas muy actualizados y entrenados para la detección temprana de incidentes.

Nada impide que se puedan calcular las reglas periódicamente y en tiempos muy cortos, bajando a una pequeña decena de minutos en vez de semanas si lo hiciera técnico especialista de seguridad. Esta es la premisa de reducción del gap de tiempo que se indicaba al principio del artículo con respecto al tiempo de ataque y la detección del mismo.

Aunque los sistemas en los que se aplica técnicas de IA están a la orden del día, es importante reseñar dos cosas:

1. **Que los sistemas de IA no son infalibles al 100 % y dependen mucho de la calidad y la cantidad de los datos con los que se entrenen**. No por disponer de muchos datos se obtienen mejores resultados si son de baja calidad y viceversa.
2. **Que la compartición de las reglas calculadas por la IA dentro de dos o más entidades, favorece la protección del conjunto de ellos. Se obtiene el típico "efecto vacuna"** que beneficia al grupo. La detección de ataques y la anticipación de contramedidas para el resto, incluso antes de sufrir dichos ataques, son los principales beneficios que se

pueden conseguir.
Para finalizar, desde mayo de 2019 las disposiciones del Reglamento 2018/1807 relativo a un marco para la libre circulación de datos no personales en la Unión Europea, ayudará a la innovación en la ciberseguridad, utilizando bases de datos comunes que fomenten el efecto “vacuna” entre entidades. Esa puede ser la línea principal de protección en no mucho tiempo.

Francisco Javier Sánchez Zurdo

AI Project Manager SIA, SISTEMAS INFORMÁTICOS ABIERTOS

computing

12 Septiembre 2019

La ciberseguridad y la posición relevante de la IA

Francisco Javier Sánchez Zurdo, desde SIA, analiza un "juego" de ataque-defensa en el que desconocemos muchas variables que ayudarían a minimizar los impactos en seguridad

Francisco Javier Sánchez Zurdo, AI Project Manager de SI

Los ataques a los sistemas informáticos de una entidad u organización son cada vez más frecuentes, tal y como estamos viendo en las últimas semanas. Acabamos de conocer impactos de diferente gravedad como el robo de información confidencial en una empresa energética o incluso el robo de millones de datos fiscales de ciudadanos y empresas de Bulgaria. Aunque existen diferentes tipologías y escalas de ataques**, gran parte de ellos se diseñan para robar credenciales de acceso o para explotar brechas de seguridad filtrando datos o solicitando rescates**. Casi nada se conoce de los impactos a pequeñas empresas o incluso a los particulares en este tipo de ataques.

En este "juego" de ataque-defensa desconocemos muchas variables que nos ayudarían a minimizar los impactos: **cuándo se realizará su ataque, qué y cómo se pretende atacar**; y fundamentalmente, cuál es la intención final del ataque. Si además añadimos que se tarda más de dos meses en descubrirse las brechas de seguridad y que se necesitan otros 50 días para contener e investigar, el escenario es totalmente negativo.

Todo lo anterior se resume en una simple frase a asumir cuanto antes:

"Siempre vamos por detrás de los malos".

Sin embargo, hay una variable de la que sí podemos tomar el control en esa situación de desventaja clara:

“El tiempo entre que se sufre un ataque y se detecta en la entidad”.

> El tiempo entre que se sufre un ataque y se detecta en la entidad es una variable que puede minimizarse con la Inteligencia Artificial

Esa es la variable que puede minimizarse con l a Inteligencia Artificial (IA).

El tiempo entre que se sufre un ataque y se detecta en la entidad es una variable que puede minimizarse con la Inteligencia Artificial

Escenarios de protección. ¿Algo nuevo?

En la actualidad se desean proteger dos escenarios distintos:

- Los sistemas de información internos en la organización: infraestructuras, servicios, activos digitales, etc.; los cuales dependen directamente de la entidad y que pueden estar on-premise o en la nube.

- La imagen y la reputación externa, que depende de la percepción que tienen terceros de la propia entidad.

No es algo nuevo que haya surgido recientemente. A modo de símil, Felipe II en su vasto imperio tuvo que contener amenazas internas (intrigas palaciegas, revuelta en Flandes, rebelión de los moriscos, …) y amenazas externas (la leyenda negra del Rey, batalla de Lepanto, …). En aquel momento se tenía un sistema polisinodial (conjunto de Consejos que trataban los asuntos de cada territorio/estado), que trasladaba los asuntos al Rey para la toma de decisiones. También tenían a su disposición una extensa red de espionaje para tener control de la información de lo que sucedía fuera del reino con respecto a los intereses del imperio.

La monitorización interna de los sistemas informáticos de una

entidad (sensores, concentradores de logs, SIEMs, …) y la monitorización externa de redes públicas/sociales /darknet son los equivalentes a día de hoy de lo que hace cinco siglos se hacía.

La IA como extractor de patrones de comportamiento

El modelo tradicional de detección de alertas se basa en el establecimiento cuasi-manual de reglas en los sistemas de monitorización por parte de los expertos analistas. Sin embargo, dichas reglas no cubren todos los casos posibles y suelen cambiar con una frecuencia mayor que la disponibilidad de los expertos para su actualización.

Con los volúmenes de datos almacenados de sistemas tipo firewall, IDS/IPS, antivirus, correos electrónicos, comunicaciones VPN, … y las noticias reputacionales monitorizadas (redes sociales principalmente), las alertas se van acumulando, siendo la mayoría de las veces falsos positivos. Esto ralentiza la contención de aquellas alertas que sí son maliciosas y que deben ser analizadas y contenidas cuanto antes.

Modelo tradicional vs Inteligencia Artificial

La IA actúa de una manera totalmente diferente. En base al histórico de actuaciones (datos y respuestas dadas en un momento determinado) y la correlación entre sistemas con el concepto de sesión de trabajo, se puede averiguar qué reglas son las que se cumplen para esos datos. La aplicación posteriormente de dichas reglas en los sistemas tradicionales de monitorización y alerta permite tener sistemas muy actualizados y entrenados para la detección temprana de incidentes.

Nada impide que se puedan calcular las reglas periódicamente y en tiempos muy cortos, bajando a una pequeña decena de minutos en vez de semanas si lo hiciera técnico especialista de seguridad. Esta es la premisa de reducción del gap de tiempo que se indicaba al principio del artículo con respecto al tiempo de ataque y la detección del mismo.

Aunque los sistemas en los que se aplica técnicas de IA están a la orden del día, es importante reseñar dos cosas:

1. **Que los sistemas de IA no son infalibles al 100%** y dependen mucho de la calidad y la cantidad de los datos con los que se entrenen. No por disponer de muchos datos se obtienen mejores resultados si son de baja calidad y viceversa.

2. **Que la compartición de las reglas calculadas por la IA dentro de dos o más entidades favorece la protección del conjunto de ellos**. Se obtiene el típico "efecto vacuna" que beneficia al grupo. La detección de ataques y la anticipación de contramedidas para el resto, incluso antes de sufrir dichos ataques, son los principales beneficios que se pueden conseguir.

Para finalizar, desde mayo de 2019 las disposiciones del Reglamento 2018/1807 relativo a un marco para la libre circulación de datos no personales en la Unión Europea, ayudará a la innovación en la ciberseguridad, utilizando bases de datos comunes que fomenten el efecto "vacuna" entre entidades. Esa puede ser la línea principal de protección en no mucho tiempo.

La ciberseguridad y la posición relevante de la IA

Por Francisco Javier Sánchez Zurdo, AI Project Manager de SIA, Sistemas Informáticos Abiertos

Los ataques a los sistemas informáticos de una entidad u organización son cada vez más frecuentes, tal y como estamos viendo en las últimas semanas. Acabamos de conocer impactos de diferente gravedad como el robo de información confidencial en una empresa energética o incluso el robo de millones de datos fiscales de ciudadanos y empresas de Bulgaria. Aunque existen diferentes tipologías y escalas de ataques, gran parte de ellos se diseñan para robar credenciales de acceso o para explotar brechas de seguridad filtrando datos o solicitando rescates. Casi nada se conoce de los impactos a pequeñas empresas o incluso a los particulares en este tipo de ataques.

En este "juego" de ataque-defensa desconocemos muchas variables que nos ayudarían a minimizar los impactos: cuándo se realizará su ataque, qué y cómo se pretende atacar; y fundamentalmente, cuál es la intención final del ataque. Si además añadimos que se tarda más de dos meses en descubrirse las brechas de seguridad y que se necesitan otros 50 días para contener e investigar, el escenario es totalmente negativo.

Todo lo anterior se resume en una simple frase a asumir cuanto antes:

"Siempre vamos por detrás de los malos".

Sin embargo, hay una variable de la que sí podemos tomar el control en esa situación de desventaja clara: "El tiempo entre que se sufre un ataque y se detecta en la entidad".

Esa es la variable que puede minimizarse con la Inteligencia Artificial (IA).

Escenarios de protección. ¿Algo nuevo?

En la actualidad se desean proteger dos escenarios distintos:

- **Los sistemas de información internos en la organización:** infraestructuras, servicios, activos digitales, etc.; los cuales dependen directamente de la entidad y que pueden estar on-premise o en la nube.
- **La imagen y la reputación externa**, que depende de la percepción que tienen terceros de la propia entidad.

No es algo nuevo que haya surgido recientemente. A modo de símil, Felipe II en su basto imperio tuvo que contener amenazas internas (intrigas palaciegas, revuelta en Flandes, rebelión de los moriscos, …) y amenazas externas (la leyenda negra del Rey, batalla de Lepanto, …). En aquel momento se tenía un sistema polisinodial (conjunto de Consejos que trataban los asuntos de cada territorio/estado), que trasladaba los asuntos al Rey para la toma de decisiones. También tenían a su disposición una extensa red de espionaje para tener control de la información de lo que sucedía fuera del reino con respecto a los intereses del imperio.
La monitorización interna de los sistemas informáticos de una entidad (sensores, concentradores de logs, SIEMs, …) y la monitorización externa de redes públicas/sociales /darknet son los equivalentes a día de hoy de lo que hace cinco siglos se hacía.

La IA como extractor de patrones de comportamiento

El modelo tradicional de detección de alertas se basa en el establecimiento cuasi-manual de reglas en los sistemas de monitorización por parte de los expertos analistas. Sin embargo, dichas reglas no cubren todos los casos posibles y suelen cambiar con una frecuencia mayor que la disponibilidad de los expertos para su actualización.
Con los volúmenes de datos almacenados de sistemas tipo firewall, IDS/IPS, antivirus, correos electrónicos, comunicaciones VPN, … y las noticias reputacionales

monitorizadas (redes sociales principalmente), las alertas se van acumulando siendo la mayoría de las veces falsos positivos. Esto ralentiza la contención de aquellas alertas que sí son maliciosas y que deben ser analizadas y contenidas cuanto antes.

La IA actúa de una manera totalmente diferente. En base al histórico de actuaciones (datos y respuestas dadas en un momento determinado) y la correlación entre sistemas con el concepto de sesión de trabajo, se puede averiguar qué reglas son las que se cumplen para esos datos. La aplicación posteriormente de dichas reglas en los sistemas tradicionales de monitorización y alerta permite tener sistemas muy actualizados y entrenados para la detección temprana de incidentes.

Nada impide que se puedan calcular las reglas periódicamente y en tiempos muy cortos, bajando a una pequeña decena de minutos en vez de semanas si lo hiciera técnico especialista de seguridad. Esta es la premisa de reducción del gap de tiempo que se indicaba al principio del artículo con respecto al tiempo de ataque y la detección del mismo. Aunque los sistemas en los que se aplica técnicas de IA están a la orden del día, es importante reseñar dos cosas:

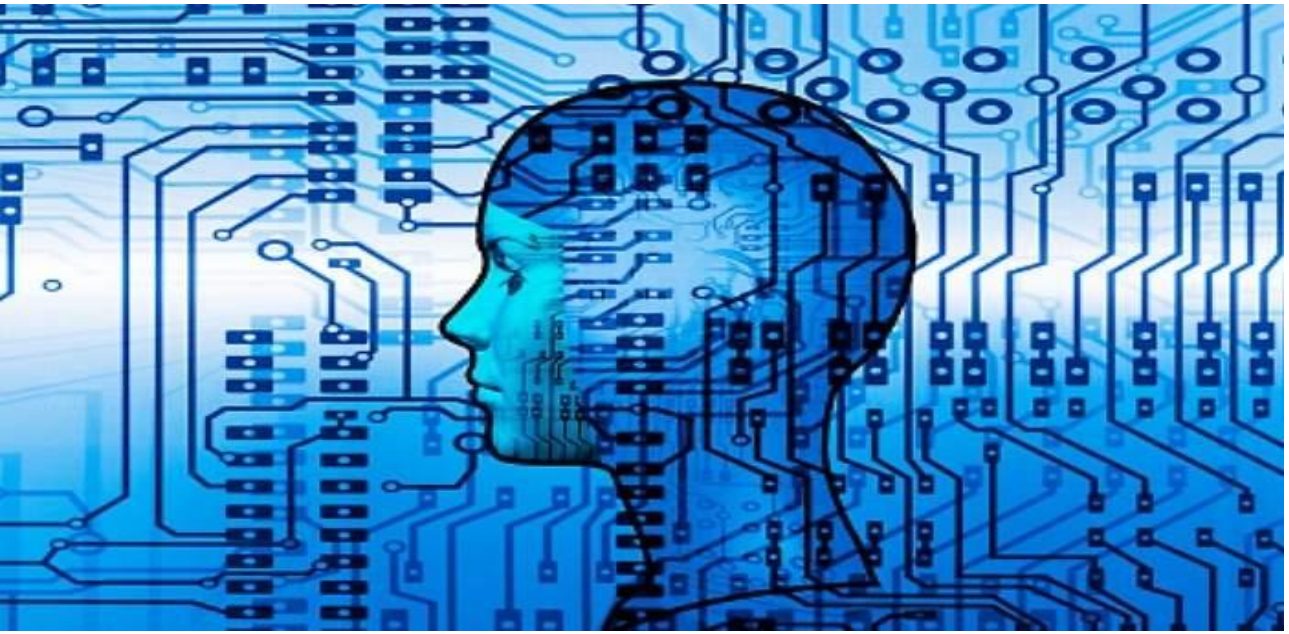
1. **Que los sistemas de IA no son infalibles al 100%** y dependen mucho de la calidad y la cantidad de los datos con los que se entrenen. No por disponer de muchos datos se obtienen mejores resultados si son de baja calidad y viceversa.
2. **Que la compartición de las reglas calculadas por la IA dentro de dos o más entidades, favorece la protección del conjunto de ellos**. Se obtiene el típico "efecto vacuna" que beneficia al grupo. La detección de ataques y la anticipación de contramedidas para el resto, incluso antes de sufrir dichos ataques, son los principales beneficios que se pueden conseguir.

Para finalizar, desde mayo de 2019 las disposiciones del Reglamento 2018/1807 relativo a un marco para la libre circulación de datos no personales en la Unión Europea, ayudará a la innovación en la ciberseguridad, utilizando bases de datos comunes que fomenten el efecto "vacuna" entre entidades. Esa puede ser la línea principal de protección en no mucho tiempo.

elEconomista.es

17 Septiembre 2019

La ciberseguridad y la posición relevante de la IA



Francisco Javier Sánchez Zurdo, AI Project Manager SIA, SISTEMAS INFORMÁTICOS ABIERTOS

Los ataques a los sistemas informáticos de una entidad u organización son cada vez más frecuentes, tal y como estamos viendo en las últimas semanas. Acabamos de conocer impactos de diferente gravedad como el robo de información confidencial en una empresa energética o incluso el robo de millones de datos fiscales de ciudadanos y empresas de Bulgaria . Aunque existen diferentes tipologías y escalas de ataques, gran parte de ellos se diseñan para robar credenciales de acceso o para explotar brechas de seguridad filtrando datos o solicitando rescates. Casi nada se conoce de los impactos a pequeñas empresas o incluso a los particulares en este tipo de ataques.

En este "juego" de ataque-defensa desconocemos muchas variables que nos ayudarían a minimizar los impactos: cuándo se realizará su ataque, qué y cómo se pretende atacar; y fundamentalmente, cuál es la intención final del ataque. Si además añadimos que se tarda más de dos meses en descubrirse las brechas de seguridad y que se necesitan otros 50 días para contener e investigar, el escenario es totalmente negativo.

Todo lo anterior se resume en una simple frase a asumir cuanto antes:

"Siempre vamos por detrás de los malos".

Sin embargo, hay una variable de la que sí podemos tomar el control en esa situación de desventaja clara:

"El tiempo entre que se sufre un ataque y se detecta en la entidad".

Esa es la variable que puede minimizarse con la Inteligencia Artificial (IA).

Escenarios de protección. ¿Algo nuevo?

En la actualidad se desean proteger dos escenarios distintos:

1. Los sistemas de información internos en la organización: infraestructuras, servicios, activos digitales, etc.; los cuales dependen directamente de la entidad y que pueden estar on-premise o en la nube.

2. La imagen y la reputación externa, que depende de la percepción que tienen terceros de la propia entidad.

No es algo nuevo que haya surgido recientemente. A modo de símil, Felipe II en su basto imperio tuvo que contener amenazas internas (intrigas palaciegas, revuelta en Flandes, rebelión de los moriscos,...) y amenazas externas (la leyenda negra del Rey, batalla de Lepanto...). En aquel momento se tenía un sistema polisinodial (conjunto de Consejos que trataban los asuntos de cada territorio/estado), que trasladaba los asuntos al Rey para la toma de decisiones. También tenían a su disposición una extensa red de espionaje para tener control de la información de lo que sucedía fuera del reino con respecto a los intereses del imperio.

La monitorización interna de los sistemas informáticos de una entidad (sensores, concentradores de logs, SIEMs...) y la monitorización externa de redes públicas/sociales /darknet son

los equivalentes a día de hoy de lo que hace cinco siglos se hacía.

La IA como extractor de patrones de comportamiento

El modelo tradicional de detección de alertas se basa en el establecimiento cuasi-manual de reglas en los sistemas de monitorización por parte de los expertos analistas. Sin embargo, dichas reglas no cubren todos los casos posibles y suelen cambiar con una frecuencia mayor que la disponibilidad de los expertos para su actualización.

Con los volúmenes de datos almacenados de sistemas tipo firewall, IDS/IPS, antivirus, correos electrónicos, comunicaciones VPN... y las noticias reputacionales monitorizadas (redes sociales principalmente), las alertas se van acumulando siendo la mayoría de las veces falsos positivos. Esto ralentiza la contención de aquellas alertas que sí son maliciosas y que deben ser analizadas y contenidas cuanto antes.

La IA actúa de una manera totalmente diferente. En base al histórico de actuaciones (datos y respuestas dadas en un momento determinado) y la correlación entre sistemas con el concepto de sesión de trabajo, se puede averiguar qué reglas son las que se cumplen para esos datos. La aplicación posteriormente de dichas reglas en los sistemas tradicionales de monitorización y alerta permite tener sistemas muy actualizados y entrenados para la detección temprana de incidentes.

Nada impide que se puedan calcular las reglas periódicamente y en tiempos muy cortos, bajando a una pequeña decena de minutos en vez de semanas si lo hiciera técnico especialista de seguridad. Esta es la premisa de reducción del gap de tiempo que se indicaba al principio del artículo con respecto al tiempo de ataque y la detección del mismo.

Aunque los sistemas en los que se aplica técnicas de IA están a la orden del día, es importante reseñar dos cosas:

1. Que los sistemas de IA no son infalibles al 100% y dependen

mucho de la calidad y la cantidad de los datos con los que se entrenen. No por disponer de muchos datos se obtienen mejores resultados si son de baja calidad y viceversa.

2. Que la compartición de las reglas calculadas por la IA dentro de dos o más entidades, favorece la protección del conjunto de ellos. Se obtiene el típico "efecto vacuna" que beneficia al grupo. La detección de ataques y la anticipación de contramedidas para el resto, incluso antes de sufrir dichos ataques, son los principales beneficios que se pueden conseguir.

Para finalizar, desde mayo de 2019 las disposiciones del Reglamento 2018/1807 relativo a un marco para la libre circulación de datos no personales en la Unión Europea, ayudará a la innovación en la ciberseguridad, utilizando bases de datos comunes que fomenten el efecto "vacuna" entre entidades. Esa puede ser la línea principal de protección en no mucho tiempo.

El servicio de Salud de Islas Baleares apuesta por la firma centralizada

Como resultado, IB-Salut dispone de un sistema que incrementa la seguridad y la productividad, a la vez que disminuye costes y el esfuerzo redundante en aras del ciudadano.

Andrea Benito

Miguel Ángel Benito, jefe de Servicio de Protección de Datos de Ib-Salut.

> "DESDE 2008, EN IB-SALUT TENEMOS DESPLEGADO EL SISTEMA DE RECETA ELECTRÓNICA"

▶ El Servicio de Salud de las Islas Baleares ha puesto en marcha dentro de su programa de estrategia de transformación digital el servicio de firma centralizada. Se trata de un sistema proporcionado por SIA que permite realizar operaciones de firma electrónica desde cualquier dispositivo informático con acceso a los certificados centralizados. Estos certificados electrónicos centralizados permiten autenticarse y firmar documentos electrónicos desde cualquier dispositivo con acceso a internet y sin ningún equipamiento adicional.

En IB-Salut se enfrentaban al reto y, a la vez, al compromiso de implantar la administración electrónica en la entidad, para lo cual necesitaban dotar a sus profesionales de certificados electrónicos reconocidos de empleado público, así como de proporcionales herramientas sencillas para la realización de firma electrónica y autenticación ante terceros organismos.

Por otro lado, tenían la necesidad de proporcionar a la dirección soluciones tecnológicas que mejorasen los tiempos en la firma del alto número de documentos que se rubrican diariamente y, además, responder a su solicitud de implantar circuitos o sistemas de firma en movilidad que les permitiera realizar la firma de documentos cuando no pudieran estar físicamente en su centro. Ya que hay que tener en cuenta la condición de esta comunidad y la distribución de los más de 150 centros que posee, tanto de atención primaria como de atención hospitalaria

y centros de administración; situación que, en ocasiones, dificulta el traslado de documentación entre los diferentes centros de Ib-Salut.

"En lo que se refiere a la implantación de sistemas de firma electrónica en el ámbito asistencial, desde 2008, en Ib-Salut tenemos desplegado el sistema de receta electrónica. Para su utilización, debíamos proporcionar a nuestros profesionales sanitarios un certificado electrónico reconocido en tarjeta criptográfica", señala Miguel Ángel Benito, jefe de Servicio de Protección de Datos del Ib-Salut. "En paralelo al funcionamiento de este sistema criptográfico, los profesionales asistenciales venían solicitando desde entonces mejoras en el proceso de firma de las recetas, que requería un tiempo mínimo de 30 a 40 segundos por cada proceso de prescripción. Como dato, en el caso de atención primaria, en la mayoría de ocasiones se realiza al menos una vez por cada paciente que atiende el profesional".

> "LA FIRMA ELECTRÓNICA HA REDUCIDO LOS TIEMPOS EN MÁS DE 30 SEGUNDOS"

Actualmente hay 3.400 profesionales con certificado centralizado que realizan diariamente 7.700 firmas (entre receta electrónica y otros procesos de negocio). En total, en agosto se han realizado 225.297 firmas, lo que ha traído consigo beneficios en la: usabilidad, independencia tecnológica, ahorro de tiempo, ahorro de costes asociados a la compra, movilidad y monitorización continua del servicio, así como seguridad jurídica.

"Respecto a las mejoras que ha supuesto para el organismo la implantación del servicio de firma centralizada, sin duda, destacaría la eliminación para los profesionales de los problemas tecnológicos y de empleo de tiempo derivados del uso de la firma en tarjeta", menciona Benito. "Desde el punto de vista asistencial, es importante resaltar la reducción de más de 30 segundos en el proceso de firma de receta electrónica, algo que permite a nuestros profesionales aumentar el tiempo de dedicación a sus pacientes, sin tener que ocuparse de problemas tecnológicos. CW

Las cuatro reglas para aumentar el compromiso del paciente

Yossi Cohen, médico ejecutivo en InterSystems y médico en NHS

Facilitar que los pacientes se comprometan con su propio cuidado mejora la salud y, también, los resultados. En este escenario, la tecnología es un facilitador clave, pero aún está en desarrollo. De hecho, la mayoría de los países muestran un nivel bajo de madurez en funciones básicas *online*, como el acceso del paciente a su HCE (Historia Clínica Electrónica), la reserva de citas o la comunicación médica mediante mensajes seguros.

Pero con tantos países con este objetivo, para conseguir el compromiso del paciente con su propio bienestar conviene tener en cuenta estas consideraciones:

1. Las objeciones de los profesionales

En septiembre de 2017, el secretario de salud del Reino Unido, Jeremy Hunt, habló de la "década del poder del paciente" y señaló: "Es la década en que se pondrá patas arriba la relación que ha existido entre médico y paciente durante tres milenios; los pacientes utilizarán la información a su alcance para ejercer un control real".

Esta mayor participación es un cambio cultural fundamental en esa relación y no siempre es fácil para los involucrados.

Los médicos deberán realinearse con esta realidad emergente y hay evidencias, en todo el mundo, de que no es sencillo. Por ejemplo, según una investigación realizada en el Reino Unido para el foro Sowerby e-Health, los médicos de cabecera son reacios a compartir datos con los pacientes. Solo uno de cada cuatro cree que los beneficios del acceso a la HCE son mayores que los riesgos.

2. Los pacientes no se impresionan fácilmente

El que los pacientes accedan a sus HCE no supone, necesariamente, un compromiso significativo. Según una investigación de las Cámaras del Parlamento, en Inglaterra, el porcentaje de consultas de médicos de cabecera que permiten el acceso al paciente, reservar citas y prescribir recetas aumentó del 3% al 97% desde 2014 a 2016. Sin embargo, solo el 0,4% de los pacientes utilizó el servicio.

Además, este acceso solo es el requisito previo para alcanzar el compromiso. El paciente debe identificar los beneficios por él mismo, más allá del acceso a su propia información.

Un obstáculo potencial es considerar las iniciativas de participación bajo el prisma del "caso de negocio" o "mejora de la atención". Los pacientes, sin embargo, lo ven bajo el prisma, "está ahí para mí", de forma que, si bien las consideraciones del proveedor son importantes, son proyectos que deben dirigirse a mantener satisfechos a los usuarios de la sanidad.

> CADA PACIENTE TIENE SUS NECESIDADES Y REQUIERE UNA FORMA DISTINTA A LA HORA DE INVOLUCRARLO

3. Elegir cuidadosamente los objetivos

Estos proyectos suelen ser el último paso en la implementación de la HCE o en la creación de un intercambio de información sanitaria. Después, los pacientes pueden acceder a las HCE, creadas como una vía para alcanzar su compromiso, pero con una experiencia de usuario único para todos.

Pero cada paciente tiene sus necesidades y requiere una forma distinta a la hora de involucrarlo. Por ejemplo, una mujer embarazada valorará un portal que le permita contactar con su médico o su matrona; localizar talleres de prenatal en su área o revisar el calendario de vacunas para el recién nacido. Por su parte, un paciente diabético querrá revisar sus análisis, enviar las últimas lecturas de glucosa en sangre a la enfermera y saber cómo controlar su enfermedad.

Por lo tanto, se debe empezar identificando los grupos de pacientes y diseñar campañas personalizadas para reforzar su compromiso. Para cada grupo, además, es importante determinar el punto óptimo de cada funcionalidad para que sea, por un lado, lo suficientemente rica para atraer al paciente y, por otro lado, lo suficientemente sencilla de implementar.

4. Adoptar una visión cauta de los beneficios

No todas las metodologías han sido tan beneficiosas como se esperaba y, a menudo, la evidencia es mixta o contradictoria. Por ejemplo: una investigación destacó casos donde los dispositivos no mejoraron la pérdida de peso durante 24 meses, las llamadas telefónicas de formación sanitaria para el paciente, combinadas con televigilancia, no redujeron los reingresos en pacientes con insuficiencia cardíaca; y los frascos de pastillas con tapones digitales no mejoraron el cumplimiento de la medicación.

Esto muestra que, cuando se decide interactuar con un grupo, es importante tener muy claro qué se desea conseguir. Es mejor adoptar una visión prudente de los beneficios mitigando riesgos con servicios que ofrezcan confianza, como la suscripción en línea o las preferencias de atención urgente. Una vez que la campaña esté activa, hay que gestionar y ajustar esa combinación según lo que funcione mejor.

Para tener éxito, los proyectos de participación de pacientes necesitan una planificación y ejecución cuidadosas, respaldadas por una buena comprensión de los diferentes grupos de pacientes y sus requisitos únicos. **CW**

elEconomista.es

29 Noviembre 2019

Javier Jarauta: "En ciberseguridad, la clave está en prevenir los ataques"

El director de Consultoría de SIA, Javier Jarauta, considera que "los ataques siempre van a existir. Aumentarán, serán cada vez más sofisticados, por lo que el reto está en la prevención".

SIA ha puesto siempre en el centro de su actividad la seguridad de sus clientes; ahora, ¿mantienen el foco en el mismo lugar?

Somos una multinacional española que este año celebra su 30º aniversario. SIA es, quizá, la mayor de las empresas especialistas en ciberseguridad tanto en cantidad como en volumen: tenemos más de 700 empleados y unos 60 millones de ingresos. Ayudamos a nuestros clientes a protegerse; trabajamos con las principales organizaciones de todos los sectores del mercado español, prácticamente desde nuestros inicios como compañía. En 1996, comenzamos con lo que antes se llamaba seguridad lógica o informática que, ahora, ha pasado a denominarse ciberseguridad.

¿Cómo se enfrenta SIA al reto de la ciberseguridad? ¿Qué sector considera que puede estar más expuesto a los ciberataques?

Los ataques siempre van a existir. Aumentarán, serán cada vez más sofisticados, por lo que el reto está en la prevención. En los primeros años de nuestra andadura, nuestro propósito era detectar lo antes posible cualquier tipo de fraude o ataque; hoy, el reto está en prevenirlos. Utilizamos personas, tecnologías y experiencias para prevenir.

Vamos siempre por detrás de los ciberdelincuentes, pero, gracias a las técnicas de Ciberinteligencia y de predicción y

prevención utilizando Inteligencia Artificial, podemos adelantarnos o, al menos, captarlos en el minuto cero del ataque. La realidad es que los delincuentes tienen muchos más medios, tiempo y dinero para atacar que nosotros para defendernos; siempre van a ir un punto por delante, pero muchas veces les ganamos adelantándonos a sus ciberataques, y ese es nuestro objetivo como especialistas.

En este sentido, las nuevas tecnologías disruptivas, sobre todo la Inteligencia Artificial, permiten que podamos predecir qué persona o proceso de la organización tiene más probabilidades de que se cometa un fraude o ciberataque contra él. De esta forma, podemos concienciarle y prepararle, intentando prever por qué vector de ataque van a tratar de entrar, si van más orientados al *phising*, al *malware* y todas sus variantes, etc. Podemos predecir este tipo de ataques para estar preparados.

En este punto, el sector financiero seguirá siendo muy atacado porque hacerlo es productivo, ya que es fácil y rápido convertir el ataque llevado a cabo en dinero. Además, hay otro factor: la banca expone sus bases de datos a internet desde hace mucho tiempo, algo que no pasa en otros sectores, y esto obliga a estas entidades a tener mayor protección. Aparte de este ámbito, los sectores industriales e infraestructuras críticas, así como las Administraciones Públicas, son los principales objetivos de la ciberdelincuencia.

¿Cómo se producen estos ataques?

Existen cientos de vectores de ataque y tipologías de ciberdelitos. Tomando como ejemplo uno de ellos, los ciberdelincuentes buscan información de los directivos y las empresas, sobre todo, a través de las redes sociales, y a partir de los datos públicos obtenidos de la entidad o persona concreta, diseñan un ataque. Está extendiéndose mucho el conocido como "El fraude del CEO"; los delincuentes se hacen pasar por uno de estos ejecutivos y envían un correo al direct financiero de la organización para que realice una transacción económica a una cuenta mulera. Al final, logran tal cantidad d datos, que generan la suficiente confianza en el empleado objetivo y consiguen que la estafa funcione. Son ataques orientados más a otros sectores que al de la banca, que está mucho más maduro y expectante con este tipo de fraudes, po lo que, tanto sus empleados como sus clientes, no son fácilmente "engañables".

En este contexto, ¿cómo se aplica la Inteligencia Artificial?
La Inteligencia Artificial utiliza datos y el aprendizaje del pasado. Se basa en el histórico, qué fraude ocurrió, qué vector utilizaron, por dónde entraron los ciberdelincuentes... Baraja algoritmos que van aprendiendo con el histórico y que previenen futuros ataques; pueden evitar, por ejemplo, que un determinado perfil de clientes sea más susceptible de ser atacado que otro y, en base a esta información, se toman medidas adicionales, como concienciación o la aplicación de mayores medidas de protección.

¿Los ataques siempre dejan huella?
Los ciberataques siempre dejan rastro, sin embargo, es muy difícil conocer el origen del mismo, asignar el ataque a una persona concreta o a un grupo determinado. Nosotros sí que accedemos al rastro ya que el sistema de detección siempre permite saber por dónde entró, cuál fue su trazabilidad, qué tácticas se utilizaron y si finalmente accedió a su objetivo o no; lo que llamamos "Ciber Kill Chain". Con este análisis, obtenemos lo más importante: aprender del ciberataque de cara al siguiente.

Con respecto a las entidades financieras, en materia de seguridad, ¿qué es lo que cree que deberían reforzar?
Depende de las tendencias. Los ciberdelincuentes intentan despistar a los que defendemos a las empresas. Últimamente, la tendencia, en lo referido al sector financiero español, ha sid un ataque con correos masivos donde roban las credenciales mediante el *phishing*, cuando antes lo hacían mediante troyanos.
En los últimos meses, España ha sido el segundo país más atacado con *phising*, sólo por detrás de Canadá. El valor de las credenciales de un usuario con una cuenta online en el mercado negro -la Internet oscura- es mucho mayor que el de una tarjeta de crédito.
Ahora, con la directiva de pagos europea PSD2 (Payment Services Directive 2), a los delincuentes se les complica la situación porque se requiere un segundo factor de autenticación que envían al móvil. No obstante, ya están buscando nuevos vectores de ataque frente a esta normativa por ejemplo, con una credencial válida cambian el número de móvil, lo suplantan y la entidad manda, sin saberlo, el segund factor de seguridad al ciberdelincuente. Es una lucha continua entre los nuevos vectores de ataque que aparecen y los nuevo

servicios de ciberseguridad que, desde SIA, diseñamos para prevenir y proteger a nuestros clientes, en los que la Inteligencia Artificial tiene un importante papel.

Usted comenta que faltan manos en nuestro país para trabajar en Ciberseguridad, ¿están haciendo algo en este sentido?

Se estima que el déficit de profesionales cualificados para 2022 en Europa será de 350.000. Es crucial formar ahora a quien ha de proteger a empresas y ciudadanos en los próximos años. Por este motivo, entre otras acciones de formación interna y en base a certificaciones, SIA colabora de forma activa y destacada en el Máster en Ciberseguridad que la Universidad Pontificia Comillas, a través de ICAI, ha puesto en marcha este curso. Y lo hace junto con otras empresas colaboradoras de otros sectores como Bankia, Iberdrola, Iberia y Santalucía.

Como compañía referente en el sector de la Ciberseguridad, con soluciones pioneras desde incluso antes del año 2000, para SIA esta acción supone aportar nuestro granito de arena al mercado laboral y a la sociedad, de reforzar nuestra atracción de talento y de avanzar en nuestra apuesta por la especialización de calidad que demanda el mercado.

"En ciberseguridad, la clave está en prevenir los ataques"

Entrevista a Javier Jarauta, director de Consultoría de SIA

El director de Consultoría de SIA, Javier Jarauta, considera que "los ataques siempre van a existir. Aumentarán, serán cada vez más sofisticados, por lo que el reto está en la prevención".

SIA ha puesto siempre en el centro de su actividad la seguridad de sus clientes; ahora, ¿mantienen el foco en el mismo lugar?

Somos una multinacional española que este año celebra su 30º aniversario. SIA es, quizá, la mayor de las empresas especialistas en ciberseguridad tanto en cantidad como en volumen: tenemos más de 700 empleados y unos 60 millones de ingresos. Ayudamos a nuestros clientes a protegerse; trabajamos con las principales organizaciones de todos los sectores del mercado español, prácticamente desde nuestros inicios como compañía. En 1996, comenzamos con lo que antes se llamaba seguridad lógica o informática que, ahora, ha pasado a denominarse ciberseguridad.

¿Cómo se enfrenta SIA al reto de la ciberseguridad? ¿Qué sector considera que puede estar más expuesto a los ciberataques?

Los ataques siempre van a existir. Aumentarán, serán cada vez más sofisticados, por lo que el reto está en la prevención. En los primeros años de nuestra andadura, nuestro propósito era detectar lo antes posible cualquier tipo de fraude o ataque; hoy, el reto está en prevenirlos. Utilizamos personas, tecnologías y experiencias para prevenir.

Vamos siempre por detrás de los ciberdelincuentes, pero, gracias a las técnicas de Ciberinteligencia y de predicción y prevención utilizando Inteligencia Artificial, podemos adelantarnos o, al menos, captarlos en el minuto cero del ataque. La realidad es que los delincuentes tienen muchos más medios, tiempo y dinero para atacar que nosotros para defendernos; siempre van a ir un punto por delante, pero muchas veces les ganamos adelantándonos a sus ciberataques,

muchas veces les ganamos adelantándonos a sus ciberataques, y ese es nuestro objetivo como especialistas.

En este sentido, las nuevas tecnologías disruptivas, sobre todo la Inteligencia Artificial, permiten que podamos predecir qué persona o proceso de la organización tiene más probabilidades de que se cometa un fraude o ciberataque contra él. De esta forma, podemos concienciarle y prepararle, intentando prever por qué vector de ataque van a tratar de entrar, si van más orientados al phising, al malware y todas sus variantes, etc Podemos predecir este tipo de ataques para estar preparados. En este punto, el sector financiero seguirá siendo muy atacado porque hacerlo es productivo, ya que es fácil y rápido convertir el ataque llevado a cabo en dinero. Además, hay otro factor: la banca expone sus bases de datos a internet desde hace mucho tiempo, algo que no pasa en otros sectores, y esto obliga a estas entidades a tener mayor protección. Aparte de este ámbito, los sectores industriales e infraestructuras críticas, así como las Administraciones Públicas, son los principales objetivos de la ciberdelincuencia.

¿Cómo se producen estos ataques?

Existen cientos de vectores de ataque y tipologías de ciberdelitos. Tomando como ejemplo uno de ellos, los ciberdelincuentes buscan información de los directivos y las empresas, sobre todo, a través de las redes sociales, y a partir de los datos públicos obtenidos de la entidad o persona concreta, diseñan un ataque. Está extendiéndose mucho el

conocido como “El fraude del CEO”; los delincuentes se hacen pasar por uno de estos ejecutivos y envían un correo al director financiero de la organización para que realice una transacción económica a una cuenta mulera. Al final, logran tal cantidad de datos, que generan la suficiente confianza en el empleado objetivo y consiguen que la estafa funcione. Son ataques orientados más a otros sectores que al de la banca, que está mucho más maduro y expectante con este tipo de fraudes, por lo que, tanto sus empleados como sus clientes, no son fácilmente ‘engañables’.

En este contexto, ¿cómo se aplica la Inteligencia Artificial?

La Inteligencia Artificial utiliza datos y el aprendizaje del pasado. Se basa en el histórico, qué fraude ocurrió, qué vector utilizaron, por dónde entraron los ciberdelincuentes... Baraja algoritmos que van aprendiendo con el histórico y que previenen futuros ataques; pueden evitar, por ejemplo, que un determinado perfil de clientes sea más susceptible de ser atacado que otro y, en base a esta información, se toman medidas adicionales, como concienciación o la aplicación de mayores medidas de protección.

¿Los ataques siempre dejan huella?

Los ciberataques siempre dejan rastro, sin embargo, es muy difícil conocer el origen del mismo, asignar el ataque a una persona concreta o a un grupo determinado. Nosotros sí que accedemos al rastro ya que el sistema de detección siempre permite saber por dónde entró, cuál fue su trazabilidad, qué tácticas se utilizaron y si finalmente accedió a su objetivo o no; lo que llamamos ‘Ciber Kill Chain’. Con este análisis, obtenemos lo más importante: aprender del ciberataque de cara al siguiente.

Con respecto a las entidades financieras, en materia de seguridad, ¿qué es lo que cree que deberían reforzar?

Depende de las tendencias. Los ciberdelincuentes intentan despistar a los que defendemos a las empresas. Últimamente, la tendencia, en lo referido al sector financiero español, ha sido un ataque con correos masivos donde roban las credenciales

mediante el phishing, cuando antes lo hacían mediante troyanos.

En los últimos meses, España ha sido el segundo país más atacado con phising, sólo por detrás de Canadá. El valor de las credenciales de un usuario con una cuenta online en el mercado negro -la internet oscura- es mucho mayor que el de una tarjeta de crédito.

Ahora, con la directiva de pagos europea PSD2 (Payment Services Directive 2), a los delincuentes se les complica la situación porque se requiere un segundo factor de autenticación que envían al móvil. No obstante, ya están buscando nuevos vectores de ataque frente a esta normativa y, por ejemplo, con una credencial válida cambian el número de móvil, lo suplantan y la entidad manda, sin saberlo, el segundo factor de seguridad al ciberdelincuente. Es una lucha continua entre los nuevos vectores de ataque que aparecen y los nuevos servicios de ciberseguridad que, desde SIA, diseñamos para prevenir y proteger a nuestros clientes, en los que la Inteligencia Artificial tiene un importante papel.

Usted comenta que faltan manos en nuestro país para trabajar en Ciberseguridad, ¿están haciendo algo en este sentido?

Se estima que el déficit de profesionales cualificados para 2022 en Europa será de 350.000. Es crucial formar ahora a quien ha de proteger a empresas y ciudadanos en los próximos años.

Por este motivo, entre otras acciones de formación interna y en base a certificaciones, SIA colabora de forma activa y destacada en el Máster en Ciberseguridad que la Universidad Pontificia Comillas, a través de ICAI, ha puesto en marcha este curso. Y lo hace junto con otras empresas colaboradoras de otros sectores como Bankia, Iberdrola, Iberia y Santalucía.

Como compañía referente en el sector de la Ciberseguridad, con soluciones pioneras desde incluso antes del año 2000, para SIA esta acción supone aportar nuestro granito de arena al mercado laboral y a la sociedad, de reforzar nuestra atracción de talento y de avanzar en nuestra apuesta por la especialización de calidad que demanda el mercado.

computing

11 Diciembre 2019

“En ciberseguridad, la clave está en prevenir los ataques”

Javier Jarauta, Director de Consultoría de SIA: “Los ataques siempre van a existir, aumentarán, serán cada vez más sofisticados, por lo que el reto está en la prevención”.

Javier Jarauta, director de consultoría de SIA

SIA ha puesto siempre en el centro de su actividad la seguridad de sus clientes; ahora, ¿mantienen el foco en el mismo lugar?

J. J.: Somos una multinacional española que este año celebra su 30º aniversario. SIA es, quizá, la mayor de las empresas especialistas en ciberseguridad tanto en cantidad como en volumen: tenemos más de 700 empleados y unos 60 millones de ingresos. Ayudamos a nuestros clientes a protegerse; trabajamos con las principales organizaciones de todos los sectores del mercado español, prácticamente desde nuestros inicios como compañía. En 1996, comenzamos con lo que antes se llamaba seguridad lógica o informática que, ahora, ha pasado a denominarse ciberseguridad.

¿Cómo se enfrenta SIA al reto de la ciberseguridad? ¿Qué sector considera que puede estar más expuesto a los ciberataques?

J. J.: Los ataques siempre van a existir. Aumentarán, serán cada vez más sofisticados, por lo que el reto está en la prevención. En los primeros años de nuestra andadura, nuestro propósito era detectar lo antes posible cualquier tipo de fraude o ataque; hoy, el reto está en prevenirlos. Utilizamos personas, tecnologías y experiencias para prevenir.

Vamos siempre por detrás de los ciberdelincuentes, pero, gracias a las técnicas de Ciberinteligencia y de predicción y prevención utilizando Inteligencia Artificial, podemos adelantarnos o, al menos, captarlos en el minuto cero del

ataque. La realidad es que los delincuentes tienen muchos más medios, tiempo y dinero para atacar que nosotros para defendernos; siempre van a ir un punto por delante, pero muchas veces les ganamos adelantándonos a sus ciberataques, y ese es nuestro objetivo como especialistas.

En este sentido, las nuevas tecnologías disruptivas, sobre todo la Inteligencia Artificial, permiten que podamos predecir qué persona o proceso de la organización tiene más probabilidades de que se cometa un fraude o ciberataque contra él. De esta forma, podemos concienciarle y prepararle, intentando prever por qué vector de ataque van a tratar de entrar, si van más orientados al phising, al malware y todas sus variantes, etc. Podemos predecir este tipo de ataques para estar preparados. En este punto, el sector financiero seguirá siendo muy atacado porque hacerlo es productivo, ya que es fácil y rápido convertir el ataque llevado a cabo en dinero. Además, hay otro factor: la banca expone sus bases de datos a internet desde hace mucho tiempo, algo que no pasa en otros sectores, y esto obliga a estas entidades a tener mayor protección. Aparte de este ámbito, los sectores industriales e infraestructuras críticas, así como las Administraciones Públicas, son los principales objetivos de la ciberdelincuencia.

Gracias a las técnicas de ciberinteligencia y de predicción y prevención utilizando Inteligencia Artificial, podemos adelantarnos o, al menos, captarlos en el minuto cero del ataque

¿Cómo se producen estos ataques?

> Gracias a las técnicas de ciberinteligencia y de predicción y prevención utilizando Inteligencia Artificial, podemos adelantarnos o, al menos, captarlos en el minuto cero del ataque

J. J.: Existen cientos de vectores de ataque y tipologías de ciberdelitos. Tomando como ejemplo uno de ellos, los ciberdelincuentes buscan información de los directivos y las empresas, sobre todo, a través de las redes sociales, y a partir de los datos públicos obtenidos de la entidad o persona concreta, diseñan un ataque. Está extendiéndose mucho el conocido como "El fraude del CEO"; los delincuentes se hacen pasar por uno de estos ejecutivos y envían un correo al director financiero de la organización para que realice una transacción económica a una cuenta mulera. Al final, logran tal cantidad de datos, que generan la suficiente confianza en el empleado objetivo y consiguen que la estafa funcione. Son ataques orientados más a otros sectores que al de la banca, que está mucho más maduro y expectante con este tipo de fraudes, por lo que, tanto sus empleados como sus clientes, no son fácilmente "engañables".

En este contexto, ¿cómo se aplica la Inteligencia Artificial?

J. J.: La Inteligencia Artificial utiliza datos y el aprendizaje del pasado. Se basa en el histórico, qué fraude ocurrió, qué vector utilizaron, por dónde entraron los ciberdelincuentes... Baraja algoritmos que van aprendiendo con el histórico y que previenen futuros ataques; pueden evitar, por ejemplo, que un determinado perfil de clientes sea más susceptible de ser atacado que otro y, en base a esta información, se toman medidas adicionales, como concienciación o la aplicación de mayores medidas de protección.

¿Los ataques siempre dejan huella?

J. J.: Los ciberataques siempre dejan rastro, sin embargo, es muy difícil conocer el origen de este, asignar el ataque a una persona concreta o a un grupo determinado. Nosotros sí que accedemos al rastro ya que el sistema de detección siempre permite saber por dónde entró, cuál fue su trazabilidad, qué tácticas se utilizaron y si finalmente accedió a su objetivo o no; lo que llamamos "Ciber Kill Chain". Con este análisis, obtenemos lo más importante: aprender del ciberataque de cara al siguiente.

Con respecto a las entidades financieras, en materia de seguridad, ¿qué es lo que cree que deberían reforzar?

J. J.: Depende de las tendencias. Los ciberdelincuentes intentan despistar a los que defendemos a las empresas. Últimamente, la tendencia, en lo referido al sector financiero español, ha sido un ataque con correos masivos donde roban las credenciales mediante el phishing, cuando antes lo hacían mediante troyanos.

En los últimos meses, España ha sido el segundo país más atacado con phising, solo por detrás de Canadá. El valor de las credenciales de un usuario con una cuenta online en el mercado negro -la internet oscura- es mucho mayor que el de una tarjeta de crédito.

Ahora, con la directiva de pagos europea PSD2 (Payment Services Directive 2), a los delincuentes se les complica la situación porque se requiere un segundo factor de autenticación que envían al móvil. No obstante, ya están buscando nuevos vectores de ataque frente a esta normativa y, por ejemplo, con una credencial válida cambian el número de móvil, lo suplantan y la entidad manda, sin saberlo, el segundo factor de seguridad al ciberdelincuente. Es una lucha continua entre los nuevos vectores de ataque que aparecen y los nuevos servicios de ciberseguridad que, desde SIA, diseñamos para prevenir y proteger a nuestros clientes, en los que la Inteligencia Artificial tiene un importante papel.

Usted comenta que faltan manos en nuestro país para trabajar en Ciberseguridad, ¿están haciendo algo en este sentido?

J. J.: Se estima que el déficit de profesionales cualificados para 2022 en Europa será de 350.000. Es crucial formar ahora a quien ha de proteger a empresas y ciudadanos en los próximos años.

Por este motivo, entre otras acciones de formación interna y en base a certificaciones, SIA colabora de forma activa y destacada en el Máster en Ciberseguridad que la Universidad Pontificia Comillas, a través de ICAI, ha puesto en marcha este curso. Y lo hace junto con otras empresas colaboradoras de otros sectores como Bankia, Iberdrola, Iberia y Santalucía.

Como compañía referente en el sector de la ciberseguridad, con soluciones pioneras desde incluso antes del año 2000, para SIA esta acción supone aportar nuestro granito de arena al mercado laboral y a la sociedad, de reforzar nuestra atracción de talento y de avanzar en nuestra apuesta por la especialización de calidad que demanda el mercado.

Entrevista a Javier Jarauta, Director de Consultoría de SIA

"En ciberseguridad, la clave está en prevenir los ataques"

El director de Consultoría de SIA, Javier Jarauta, considera que "los ataques siempre van a existir. Aumentarán, serán cada vez más sofisticados, por lo que el reto está en la prevención".

1.- SIA ha puesto siempre en el centro de su actividad la seguridad de sus clientes; ahora, ¿mantienen el foco en el mismo lugar?

Somos una multinacional española que este año celebra su 30º aniversario. SIA es, quizá, la mayor de las empresas especialistas en ciberseguridad tanto en cantidad como en volumen: tenemos más de 700 empleados y unos 60 millones de ingresos. Ayudamos a nuestros clientes a protegerse; trabajamos con las principales organizaciones de todos los sectores del mercado español, prácticamente desde nuestros inicios como compañía. En 1996, comenzamos con lo que antes se llamaba seguridad lógica o informática que, ahora, ha pasado a denominarse ciberseguridad.

2.- ¿Cómo se enfrenta SIA al reto de la ciberseguridad? ¿Qué sector considera que puede estar más expuesto a los ciberataques?

Los ataques siempre van a existir. Aumentarán, serán cada vez más sofisticados, por lo que el reto está en la prevención. En los primeros años de nuestra andadura, nuestro propósito era detectar lo antes posible cualquier tipo de fraude o ataque; hoy, el reto está en prevenirlos. Utilizamos personas, tecnologías y experiencias para prevenir.

Vamos siempre por detrás de los ciberdelincuentes, pero, gracias a las técnicas de Ciberinteligencia y de predicción y prevención utilizando Inteligencia Artificial, podemos adelantarnos o, al menos, captarlos en el minuto cero del ataque. La realidad es que los delincuentes tienen muchos más medios, tiempo y dinero para atacar que nosotros para defendernos; siempre van a ir un punto por

delante, pero muchas veces les ganamos adelantándonos a sus ciberataques, y ese es nuestro objetivo como especialistas.
En este sentido, las nuevas tecnologías disruptivas, sobre todo la Inteligencia Artificial, permiten que podamos predecir qué persona o proceso de la organización tiene más probabilidades de que se cometa un fraude o ciberataque contra él. De esta forma, podemos concienciarle y prepararle, intentando prever por qué vector de ataquevan a tratar de entrar, si van más orientados al phising, al malware y todas sus variantes, etc Podemos predecir este tipo de ataques para estar preparados. En este punto, el sector financiero seguirá siendo muy atacado porque hacerlo es productivo, ya que es fácil y rápido convertir el ataque llevado a cabo en dinero. Además, hay otro factor: la banca expone sus bases de datos a internet desde hace mucho tiempo, algo que no pasa en otros sectores, y esto obliga a estas entidades a tener mayor protección. Aparte de este ámbito, los sectores industriales e infraestructuras críticas, así como las Administraciones Públicas, son los principales objetivos de la ciberdelincuencia.

3.- ¿Cómo se producen estos ataques?

Existen cientos de vectores de ataque y tipologías de ciberdelitos. Tomando como ejemplo uno de ellos, los ciberdelincuentes buscan información de los directivos y las empresas, sobre todo, a través de las redes sociales, y a partir de los datos públicos obtenidos de la entidad o persona concreta, diseñan un ataque. Está extendiéndose mucho el conocido como “El fraude del CEO”; los delincuentes se hacen pasar por uno de estos ejecutivos y envían un correo al director financiero de la organización para que realice una transacción económica a una cuenta mulera. Al final, logran tal cantidad de datos, que generan la suficiente confianza en el empleado objetivo y consiguen que la estafa funcione. Son ataques orientados más a otros sectores que al de la banca, que está mucho más maduro y expectante con este tipo de fraudes, por lo que, tanto sus empleados como sus clientes, no son fácilmente “engañables”.

4.- En este contexto, ¿cómo se aplica la Inteligencia Artificial?

La Inteligencia Artificial utiliza datos y el aprendizaje del pasado. Se basa en el histórico, qué fraude ocurrió, qué vector utilizaron, por dónde entraron los ciberdelincuentes... Baraja algoritmos que van aprendiendo con el histórico y que previenen futuros ataques; pueden evitar, por ejemplo, que un determinado perfil de clientes sea más susceptible de ser atacado que otro y, en base a esta información, se toman medidas adicionales, como concienciación o la aplicación de mayores medidas de protección.

5.- ¿Los ataques siempre dejan huella?

Los ciberataques siempre dejan rastro, sin embargo, es muy difícil conocer el origen del mismo, asignar el ataque a una persona concreta o a un grupo determinado. Nosotros sí que accedemos al rastro ya que el sistema de detección siempre permite saber por dónde entró, cuál fue su trazabilidad, qué tácticas se utilizaron y si finalmente accedió a su objetivo o no; lo que llamamos "Ciber Kill Chain". Con este análisis, obtenemos lo más importante: aprender del ciberataque de cara al siguiente.

6.- Con respecto a las entidades financieras, en materia de seguridad, ¿qué es lo que cree que deberían reforzar?

Depende de las tendencias. Los ciberdelincuentes intentan despistar a los que defendemos a las empresas. Últimamente, la tendencia, en lo referido al sector financiero español, ha sido un ataque con correos masivos donde roban las credenciales mediante el phishing, cuando antes lo hacían mediante troyanos.
En los últimos meses, España ha sido el segundo país más atacado con phising, sólo por detrás de Canadá. El valor de las credenciales de un usuario con una cuenta online en el mercado negro -la internet oscura- es mucho mayor que el de una tarjeta de crédito.
Ahora, con la directiva de pagos europea PSD2 (Payment Services Directive 2), a los delincuentes se les complica la situación porque se requiere un segundo factor de autenticación que envían al móvil. No obstante, ya están

buscando nuevos vectores de ataque frente a esta normativa y, por ejemplo, con una credencial válida cambian el número de móvil, lo suplantan y la entidad manda, sin saberlo, el segundo factor de seguridad al ciberdelincuente. Es una lucha continua entre los nuevos vectores de ataque que aparecen y los nuevos servicios de ciberseguridad que, desde SIA, diseñamos para prevenir y proteger a nuestros clientes, en los que la Inteligencia Artificial tiene un importante papel.

7.- Usted comenta que faltan manos en nuestro país para trabajar en Ciberseguridad, ¿están haciendo algo en este sentido?

Se estima que el déficit de profesionales cualificados para 2022 en Europa será de 350.000. Es crucial formar ahora a quien ha de proteger a empresas y ciudadanos en los próximos años.

Por este motivo, entre otras acciones de formación interna y en base a certificaciones, SIA colabora de forma activa y destacada en el Máster en Ciberseguridad que la Universidad Pontificia Comillas, a través de ICAI, ha puesto en marcha este curso. Y lo hace junto con otras empresas colaboradoras de otros sectores como Bankia, Iberdrola, Iberia y Santalucía.

Como compañía referente en el sector de la Ciberseguridad, con soluciones pioneras desde incluso antes del año 2000, para SIA esta acción supone aportar nuestro granito de arena al mercado laboral y a la sociedad, de reforzar nuestra atracción de talento y de avanzar en nuestra apuesta por la especialización de calidad que demanda el mercado.

4.- En este contexto, ¿cómo se aplica la Inteligencia Artificial?

La Inteligencia Artificial utiliza datos y el aprendizaje del pasado. Se basa en el histórico, qué fraude ocurrió, qué vector utilizaron, por dónde entraron los ciberdelincuentes... Baraja algoritmos que van aprendiendo con el histórico y que previenen futuros ataques; pueden evitar, por ejemplo, que un determinado perfil de clientes sea más susceptible de ser atacado que otro y, en base a esta información, se toman medidas adicionales, como concienciación o la aplicación de mayores medidas de protección.

5.- ¿Los ataques siempre dejan huella?

Los ciberataques siempre dejan rastro, sin embargo, es muy difícil conocer el origen del mismo, asignar el ataque a una persona concreta o a un grupo determinado. Nosotros sí que accedemos al rastro ya que el sistema de detección siempre permite saber por dónde entró, cuál fue su trazabilidad, qué tácticas se utilizaron y si finalmente accedió a su objetivo o no; lo que llamamos "Ciber Kill Chain". Con este análisis, obtenemos lo más importante: aprender del ciberataque de cara al siguiente.

6.- Con respecto a las entidades financieras, en materia de seguridad, ¿qué es lo que cree que deberían reforzar?

Depende de las tendencias. Los ciberdelincuentes intentan despistar a los que defendemos a las empresas. Últimamente, la tendencia, en lo referido al sector financiero español, ha sido un ataque con correos masivos donde roban las credenciales mediante el phishing, cuando antes lo hacían mediante troyanos.
En los últimos meses, España ha sido el segundo país más atacado con phising, sólo por detrás de Canadá. El valor de las credenciales de un usuario con una cuenta online en el mercado negro -la internet oscura- es mucho mayor que el de una tarjeta de crédito.
Ahora, con la directiva de pagos europea PSD2 (Payment Services Directive 2), a los delincuentes se les complica la situación porque se requiere un segundo factor de autenticación que envían al móvil. No obstante, ya están buscando nuevos vectores de ataque frente a esta

El fraude del CEO: cuando los más preparados también caen…

Personas y empresas estamos inmersos en una sociedad que sufre una transformación digital exponencial e implica la aparición continua de nuevas y grandes oportunidades, pero también de nuevos riesgos y fraudes. En esta vorágine tecnológica, hemos de ser conscientes que muchos de los fraudes que sufrimos por internet no dejan de ser adaptaciones de las estafas clásicas del mundo físico. Parece mentira, pero los timos más rentables, según datos actuales de la Policía y Guardia Civil, siguen siendo los más simples: el inspector del gas, el tocomocho, la estampita, etc. Ahora también son llamados de tipo “Low-Tech”.

En Internet viene a pasar algo similar, las estafas que atacan directamente al comportamiento de las personas son de las más productivas para los ciberdelincuentes. Este es el caso de lo que denominamos el fraude del CEO (Chief Executive Officer) o también conocido por otros nombres tan significativos como “Whaling” (Whale-Phising: pesca del pez gordo) o lo que en términos técnicos catalogamos como BEC (Business Email Compromise).

El impacto que tiene este tipo de fraude en la sociedad es más alto de lo que imaginamos y los datos que aportan los diferentes organismos internacionales que vigilan el cibercrimen son aterradores.

El FBI en su sección IC3 (Internet Crime Complaint Center) estima un fraude de 12.500 millones de dólares en

los últimos 5 años, con 78.000 casos identificados. Europol y la Unidad de Inteligencia Financiera Americana FinCEN mencionan cifras de 300 millones de dólares como media de fraude al mes durante 2018.

Aunque no existen datos consolidados a nivel español, solamente bastan dos hechos recientes que nos deben poner bajo alerta. El fraude a la Empresa Municipal de Transporte EMT de Valencia, de 4 millones de euros durante septiembre de 2019 y la detención por parte de la Guardia Civil en la operación Lavanco de 3 residentes en España por estafar mediante el fraude del CEO un total de 10 millones de euros a 12 empresas en 10 países extranjeros.

Lo más llamativo de esta estafa es que va dirigida a empresas de todo tipo y sector. Además los empleados que caen en el fraude pueden ser grandes profesionales en su puesto, concienciados y despiertos, pero el arte de engañar de los cibercriminales es superior.

La acción de los "cibermalos" se centra en estafar a empleados para que realicen pagos fraudulentos a una tercera parte no autorizada, pensando que quien se lo ordena con urgencia y confidencialidad es uno de sus superiores jerárquicos, al que han suplantado previamente.

En una primera fase, los cibercriminales estudian a fondo la empresa y a sus directivos, como el CEO o el CFO, hasta obtener cuentas de correo electrónico válidas y otros importantes datos de la organización. Explotan la inmensa información personal y empresarial que todos dejamos en las redes sociales (Ingeniería Social).

En la tercera fase del fraude del CEO se utilizan técnicas de presión por urgencia, confidencialidad, simulando confianza entre emisor y remitente

En la segunda fase, utilizando la información conseguida se envían correos electrónicos falsos con instrucciones para realizar transferencias o envío de información confidencial a cuentas fraudulentas.

En la tercera fase, para que el empleado ejecute la transacción a la cuenta de los ciberdelincuentes, utilizan

técnicas de presión por urgencia, confidencialidad, simulando confianza entre emisor y remitente. Una vez realizada la transferencia, hacen desaparecer dicho dinero inmediatamente.

Este procedimiento de actuación tiene múltiples variantes, pero lo importante es conocer y concienciar a todos los empleados sobre la existencia de esta estafa y cómo prevenirla y detectarla. Una de las mejores maneras de protegerse dentro de una organización es, por tanto, poner en marcha planes de concienciación o persuasión, basados principalmente en:

•Sospechar siempre de correos con asuntos muy utilizados por este tipo de fraude, como “Important”, “Confidential” o “Notification of payment received”.

•Observar muy bien las direcciones origen de los correos sospechosos.

•Implantar procedimientos de doble verificación en la empresa entre personas y sistemas de doble factor de autenticación.

•Utilizar sistemas de gestión de la identidad y de firma electrónica para autenticación fuerte de los usuarios.

•Realizar planes de concienciación y persuasión continuos en la organización.

•Disponer de servicios avanzados de prevención y detección temprana.

•Diseñar y entrenar procedimientos de respuesta ante incidentes y planes de resiliencia.

El futuro que nos espera con el fraude del CEO es complejo y peligroso. El mal ha existido siempre y existirá. El “cibermal” además está potenciado por una sociedad global con un ritmo frenético. Sin embargo el conocimiento, la formación e información puede ser nuestro salvavidas. La persona, que es el eslabón más débil de la ciberseguridad, es, a su vez, la defensa más fuerte contra los ciberataques que nos depara el futuro. Personas con principios y empresas especializadas en este ámbito, siempre estaremos aquí para defender a nuestra sociedad, adaptándonos al ritmo de los tiempos.

Por Javier Jarauta, Director de consultoría de SIA.

computing

17 Diciembre 2019

El fraude del CEO. Los más preparados también caen…

Por Javier Jarauta, Director de consultoría de SIA.

Javier Jarauta, Director de Consultoría de SIA

Personas y empresas estamos inmersos en una sociedad que sufre una transformación digital exponencial e implica la aparición continua de nuevas y grandes oportunidades, pero también de nuevos riesgos y fraudes.

En esta vorágine tecnológica, **hemos de ser conscientes que muchos de los fraudes que sufrimos por Internet no dejan de ser adaptaciones de las estafas clásicas del mundo físico.** Parece mentira, pero los timos más rentables, según datos actuales de la Policía y Guardia Civil, siguen siendo los más simples: el inspector del gas, el tocomocho, la estampita, etc. Ahora también son llamados de tipo 'Low-Tech'.

En Internet viene a pasar algo similar, las estafas que atacan directamente al comportamiento de las personas son de las más productivas para los ciberdelincuentes. Este es el caso de lo que denominamos el fraude del CEO (Chief Executive Officer) o también conocido por otros nombres tan significativos como 'Whaling' (Whale-Phising: pesca del pez gordo) o lo que en términos técnicos catalogamos como BEC (Business Email Compromise).

El impacto que tiene este tipo de fraude en la sociedad es más alto de lo que imaginamos y los datos que aportan los diferentes organismos internacionales que vigilan el cibercrimen son aterradores.

El FBI en su sección IC3 (Internet Crime Complaint Center) estima un fraude de 12.500 millones de dólares en los últimos 5 años, con 78.000 casos identificados. Europol y la Unidad de Inteligencia Financiera Americana FinCEN mencionan cifras de

300 millones de dólares como media de fraude al mes durante 2018.

Aunque no existen datos consolidados a nivel español, solamente bastan dos hechos recientes que nos deben poner bajo alerta. El fraude a la Empresa Municipal de Transporte EMT de Valencia, de 4 millones de euros durante septiembre de 2019 y la detención por parte de la Guardia Civil en la operación Lavanco de tres residentes en España por estafar mediante el fraude del CEO un total de 10 millones de euros a 12 empresas en 10 países extranjeros.

> La acción de los ‘cibermalos’ se centra en estafar a empleados para que realicen pagos fraudulentos a una tercera parte no autorizada, pensando que quien se lo ordena es uno de sus superiores jerárquicos

La acción de los ‘cibermalos’ se centra en estafar a empleados para que realicen pagos fraudulentos a una tercera parte no autorizada, pensando que quien se lo ordena es uno de sus superiores jerárquicos
Lo más llamativo de esta estafa es que va dirigida a empresas de todo tipo y sector. Además, los empleados que caen en el fraude pueden ser grandes profesionales en su puesto, concienciados y despiertos, pero el arte de engañar de los cibercriminales es superior.

La acción de los ‘cibermalos’ se centra en estafar a empleados para que realicen pagos fraudulentos a una tercera parte no autorizada, pensando que quien se lo ordena con urgencia y confidencialidad es uno de sus superiores jerárquicos, al que han suplantado previamente.

En una primera fase, los cibercriminales estudian a fondo la empresa y a sus directivos, como el CEO o el CFO, hasta obtener cuentas de correo electrónico válidas y otros importantes datos de la organización. Explotan la inmensa información personal y empresarial que todos dejamos en las redes sociales (Ingeniería Social).

En la segunda fase, utilizando la información conseguida se envían correos electrónicos falsos con instrucciones para realizar transferencias o envío de información confidencial a cuentas fraudulentas.

En la tercera fase, para que el empleado ejecute la transacción a la cuenta de los ciberdelincuentes, utilizan técnicas de presión por urgencia, confidencialidad, simulando confianza entre emisor y remitente. Una vez realizada la transferencia, hacen desaparecer dicho dinero inmediatamente.

Este procedimiento de actuación tiene múltiples variantes, pero lo importante es conocer y concienciar a todos los empleados sobre la existencia de esta estafa y cómo prevenirla y detectarla. Una de las mejores maneras de protegerse dentro de una organización es, por tanto, poner en marcha planes de concienciación o persuasión, basados principalmente en:

- Sospechar siempre de correos con asuntos muy utilizados por este tipo de fraude, como ‘Important’, ‘Confidential’ o ‘Notification of payment received’.

- Observar muy bien las direcciones origen de los correos sospechosos.

- Implantar procedimientos de doble verificación en la empresa entre personas y sistemas de doble factor de autenticación.

- **Utilizar sistemas de gestión de la identidad** y de firma electrónica para autenticación fuerte de los usuarios.

- Realizar planes de concienciación y persuasión continuos en la organización.

- Disponer de servicios avanzados de prevención y detección temprana.

- Diseñar y entrenar procedimientos de respuesta ante incidentes y planes de resiliencia.

El futuro que nos espera con el fraude del CEO es complejo y peligroso. El mal ha existido siempre y existirá. El 'cibermal' además está potenciado por una sociedad global con un ritmo frenético. Sin embargo, el conocimiento, la formación e información puede ser nuestro salvavidas. La persona, que es el eslabón más débil de la ciberseguridad, es, a su vez, la defensa más fuerte contra los ciberataques que nos depara el futuro. Personas con principios y empresas especializadas en este ámbito, siempre estaremos aquí para defender a nuestra sociedad, adaptándonos al ritmo de los tiempos.

elEconomista.es

19 Diciembre 2019

"En ciberseguridad, la clave está en prevenir los ataques"

El director de Consultoría de SIA, Javier Jarauta, considera que "los ataques siempre van a existir. Aumentarán, serán cada vez más sofisticados, por lo que el reto está en la prevención".

SIA ha puesto siempre en el centro de su actividad la seguridad de sus clientes; ahora, ¿mantienen el foco en el mismo lugar?

Somos una multinacional española que este año celebra su 30º aniversario. SIA es, quizá, la mayor de las empresas especialistas en ciberseguridad tanto en cantidad como en volumen: tenemos más de 700 empleados y unos 60 millones de ingresos. Ayudamos a nuestros clientes a protegerse; trabajamos con las principales organizaciones de todos los sectores del mercado español, prácticamente desde nuestros inicios como compañía. En 1996, comenzamos con lo que antes se llamaba seguridad lógica o informática que, ahora, ha pasado a denominarse ciberseguridad.

¿Cómo se enfrenta SIA al reto de la ciberseguridad? ¿Qué sector considera que puede estar más expuesto a los ciberataques?

Los ataques siempre van a existir. Aumentarán, serán cada vez más sofisticados, por lo que el reto está en la prevención. En los primeros años de nuestra andadura, nuestro propósito era detectar lo antes posible cualquier tipo de fraude o ataque; hoy, el reto está en prevenirlos. Utilizamos personas, tecnologías y experiencias para prevenir.

Vamos siempre por detrás de los ciberdelincuentes, pero, gracias a las técnicas de Ciberinteligencia y de predicción y

prevención utilizando Inteligencia Artificial, podemos adelantarnos o, al menos, captarlos en el minuto cero del ataque. La realidad es que los delincuentes tienen muchos más medios, tiempo y dinero para atacar que nosotros para defendernos; siempre van a ir un punto por delante, pero muchas veces les ganamos adelantándonos a sus ciberataques, y ese es nuestro objetivo como especialistas.

En este sentido, las nuevas tecnologías disruptivas, sobre todo la Inteligencia Artificial, permiten que podamos predecir qué persona o proceso de la organización tiene más probabilidades de que se cometa un fraude o ciberataque contra él. De esta forma, podemos concienciarle y prepararle, intentando prever por qué vector de ataque van a tratar de entrar, si van más orientados al *phising*, al *malware* y todas sus variantes, etc. Podemos predecir este tipo de ataques para estar preparados.

En este punto, el sector financiero seguirá siendo muy atacado porque hacerlo es productivo, ya que es fácil y rápido convertir el ataque llevado a cabo en dinero. Además, hay otro factor: la banca expone sus bases de datos a internet desde hace mucho tiempo, algo que no pasa en otros sectores, y esto obliga a estas entidades a tener mayor protección. Aparte de este ámbito, los sectores industriales e infraestructuras críticas, así como las Administraciones Públicas, son los principales objetivos de la ciberdelincuencia.

¿Cómo se producen estos ataques?

Existen cientos de vectores de ataque y tipologías de ciberdelitos. Tomando como ejemplo uno de ellos, los ciberdelincuentes buscan información de los directivos y las empresas, sobre todo, a través de las redes sociales, y a partir de los datos públicos obtenidos de la entidad o persona concreta, diseñan un ataque. Está extendiéndose mucho el conocido como "El fraude del CEO"; los delincuentes se hacen pasar por uno de estos ejecutivos y envían un correo al directo financiero de la organización para que realice una transacción económica a una cuenta mulera. Al final, logran tal cantidad d datos, que generan la suficiente confianza en el empleado objetivo y consiguen que la estafa funcione. Son ataques orientados más a otros sectores que al de la banca, que está mucho más maduro y expectante con este tipo de fraudes, po lo que, tanto sus empleados como sus clientes, no son fácilmente "engañables".

En este contexto, ¿cómo se aplica la Inteligencia Artificial?
La Inteligencia Artificial utiliza datos y el aprendizaje del pasado. Se basa en el histórico, qué fraude ocurrió, qué vector utilizaron, por dónde entraron los ciberdelincuentes... Baraja algoritmos que van aprendiendo con el histórico y que previenen futuros ataques; pueden evitar, por ejemplo, que un determinado perfil de clientes sea más susceptible de ser atacado que otro y, en base a esta información, se toman medidas adicionales, como concienciación o la aplicación de mayores medidas de protección.

¿Los ataques siempre dejan huella?
Los ciberataques siempre dejan rastro, sin embargo, es muy difícil conocer el origen del mismo, asignar el ataque a una persona concreta o a un grupo determinado. Nosotros sí que accedemos al rastro ya que el sistema de detección siempre permite saber por dónde entró, cuál fue su trazabilidad, qué tácticas se utilizaron y si finalmente accedió a su objetivo o no; lo que llamamos "Ciber Kill Chain". Con este análisis, obtenemos lo más importante: aprender del ciberataque de cara al siguiente.

Con respecto a las entidades financieras, en materia de seguridad, ¿qué es lo que cree que deberían reforzar?
Depende de las tendencias. Los ciberdelincuentes intentan despistar a los que defendemos a las empresas. Últimamente, la tendencia, en lo referido al sector financiero español, ha sid un ataque con correos masivos donde roban las credenciales mediante el *phishing*, cuando antes lo hacían mediante troyanos.
En los últimos meses, España ha sido el segundo país más atacado con *phising*, sólo por detrás de Canadá. El valor de las credenciales de un usuario con una cuenta online en el mercado negro -la Internet oscura- es mucho mayor que el de una tarjeta de crédito.
Ahora, con la directiva de pagos europea PSD2 (Payment Services Directive 2), a los delincuentes se les complica la situación porque se requiere un segundo factor de autenticación que envían al móvil. No obstante, ya están buscando nuevos vectores de ataque frente a esta normativa por ejemplo, con una credencial válida cambian el número de móvil, lo suplantan y la entidad manda, sin saberlo, el segund factor de seguridad al ciberdelincuente. Es una lucha continua entre los nuevos vectores de ataque que aparecen y los nuevo

servicios de ciberseguridad que, desde SIA, diseñamos para prevenir y proteger a nuestros clientes, en los que la Inteligencia Artificial tiene un importante papel.

Usted comenta que faltan manos en nuestro país para trabajar en Ciberseguridad, ¿están haciendo algo en este sentido?

Se estima que el déficit de profesionales cualificados para 2022 en Europa será de 350.000. Es crucial formar ahora a quien ha de proteger a empresas y ciudadanos en los próximos años. Por este motivo, entre otras acciones de formación interna y en base a certificaciones, SIA colabora de forma activa y destacada en el Máster en Ciberseguridad que la Universidad Pontificia Comillas, a través de ICAI, ha puesto en marcha este curso. Y lo hace junto con otras empresas colaboradoras de otros sectores como Bankia, Iberdrola, Iberia y Santalucía.

Como compañía referente en el sector de la Ciberseguridad, con soluciones pioneras desde incluso antes del año 2000, para SIA esta acción supone aportar nuestro granito de arena al mercado laboral y a la sociedad, de reforzar nuestra atracción de talento y de avanzar en nuestra apuesta por la especialización de calidad que demanda el mercado.

elEconomista.es

23 Diciembre 2019

El fraude del CEO: los más preparados también caen...

Por Javier Jarauta, director de consultoría de SIA.

Personas y empresas estamos inmersos en una sociedad que sufre una transformación digital exponencial e implica la aparición continua de nuevas y grandes oportunidades, pero también de nuevos riesgos y fraudes.

En esta vorágine tecnológica, hemos de ser conscientes que muchos de los fraudes que sufrimos por Internet no dejan de ser adaptaciones de las estafas clásicas del mundo físico.

Parece mentira, pero los timos más rentables, según datos actuales de la Policía y Guardia Civil, siguen siendo los más simples: el inspector del gas, el tocomocho, la estampita, etc. Ahora también son llamados de tipo "Low-Tech".

En Internet viene a pasar algo similar, las estafas que atacan directamente al comportamiento de las personas son de las más productivas para los ciberdelincuentes. Este es el caso de lo que denominamos el fraude del CEO (Chief Executive Officer) o también conocido por otros nombres tan significativos como "Whaling" (Whale-Phising: pesca del pez gordo) o lo que en términos técnicos catalogamos como BEC (Business Email Compromise).

El impacto que tiene este tipo de fraude en la sociedad es más alto de lo que imaginamos y los datos que aportan los diferentes organismos internacionales que vigilan el cibercrimen son aterradores.

El FBI (1) en su sección IC3 (Internet Crime Complaint Center) estima un fraude de 12.500 millones de dólares en los últimos 5 años, con 78.000 casos identificados. Europol (2) y la Unidad de Inteligencia Financiera Americana FinCEN mencionan cifras de 300 millones de dólares como media de fraude al mes durante 2018.

Aunque no existen datos consolidados a nivel español, solamente bastan dos hechos recientes que nos deben poner bajo alerta. El fraude a la Empresa Municipal de Transporte EMT de Valencia (3), de 4 millones de euros durante septiembre de 2019 y la detención por parte de la Guardia Civil (4) en la operación Lavanco de 3 residentes en España por estafar mediante el fraude del CEO un total de 10 millones de euros a 12 empresas en 10 países extranjeros.

Lo más llamativo de esta estafa es que va dirigida a empresas

de todo tipo y sector. Además los empleados que caen en el fraude pueden ser grandes profesionales en su puesto, concienciados y despiertos, pero el arte de engañar de los cibercriminales es superior.

La acción de los "cibermalos" se centra en estafar a empleados para que realicen pagos fraudulentos a una tercera parte no autorizada, pensando que quien se lo ordena con urgencia y confidencialidad es uno de sus superiores jerárquicos, al que han suplantado previamente.

En una primera fase, los cibercriminales estudian a fondo la empresa y a sus directivos, como el CEO o el CFO, hasta obtener cuentas de correo electrónico válidas y otros importantes datos de la organización. Explotan la inmensa información personal y empresarial que todos dejamos en las redes sociales (Ingeniería Social).

En la segunda fase, utilizando la información conseguida se envían correos electrónicos falsos con instrucciones para realizar transferencias o envío de información confidencial a cuentas fraudulentas.

En la tercera fase, para que el empleado ejecute la transacción a la cuenta de los ciberdelincuentes, utilizan técnicas de presión por urgencia, confidencialidad, simulando confianza entre emisor y remitente. Una vez realizada la transferencia, hacen desaparecer dicho dinero inmediatamente.

Este procedimiento de actuación tiene múltiples variantes, pero lo importante es conocer y concienciar a todos los empleados sobre la existencia de esta estafa y cómo prevenirla y detectarla. Una de las mejores maneras de protegerse dentro de una organización es, por tanto, poner en marcha planes de concienciación o persuasión, basados principalmente en:

- Sospechar siempre de correos con asuntos muy utilizados por este tipo de fraude, como "Important", "Confidential" o "Notification of payment received".
- Observar muy bien las direcciones origen de los correos sospechosos.
- Implantar procedimientos de doble verificación en la empresa entre personas y sistemas de doble factor de autenticación.
- Utilizar sistemas de gestión de la identidad y de firma electrónica para autenticación fuerte de los usuarios.
- Realizar planes de concienciación y persuasión continuos en la organización.
- Disponer de servicios avanzados de prevención y detección

temprana.
- Diseñar y entrenar procedimientos de respuesta ante incidentes y planes de resiliencia.

El futuro que nos espera con el fraude del CEO es complejo y peligroso. El mal ha existido siempre y existirá. El "cibermal" además está potenciado por una sociedad global con un ritmo frenético. Sin embargo el conocimiento, la formación e información puede ser nuestro salvavidas. La persona, que es el eslabón más débil de la ciberseguridad, es, a su vez, la defensa más fuerte contra los ciberataques que nos depara el futuro. Personas con principios y empresas especializadas en este ámbito, siempre estaremos aquí para defender a nuestra sociedad, adaptándonos al ritmo de los tiempos.

elEconomista.es

23 Diciembre 2019

tribuna

El fraude del CEO. Los más preparados también caen...

Personas y empresas estamos inmersos en una transformación digital exponencial que implica la aparición continua de nuevas oportunidades, pero también de nuevos riesgos y fraudes

Javier Jarauta
Director de consultoría de SIA

En esta vorágine tecnológica, hemos de ser conscientes que muchos de los fraudes que sufrimos por internet no dejan de ser adaptaciones de las estafas clásicas del mundo físico. Parece mentira, pero los timos más rentables, según datos actuales de la Policía y Guardia Civil, siguen siendo los más simples: el inspector del gas, el tocomocho, la estampita, etc. Ahora también son llamados de tipo *Low-Tech*.

En Internet viene a pasar algo similar, las estafas que atacan directamente al comportamiento de las personas son de las más productivas para los ciberdelincuentes. Este es el caso de lo que denominamos el fraude del CEO (Chief Executive Officer) o también conocido por otros nombres tan significativos como *Whaling* (*Whale-Phising*: pesca del pez gordo) o lo que en términos técnicos catalogamos como BEC -*Business Email Compromise*-.

El impacto que tiene este tipo de fraude en la sociedad es más alto de lo que imaginamos y los datos que aportan los diferentes organismos internacionales que vigilan el cibercrimen son aterradores.

El FBI (1) en su sección IC3 -*Internet Crime ComplaintCenter*- estima un fraude de 12.500 millones de dólares en los últimos cinco años, con 78.000 casos identificados. Europol (2) y la Unidad de Inteligencia Financiera Americana FinCEN mencionan cifras de 300 millones de dólares como media de fraude al mes durante 2018.

Aunque no existen datos consolidados a nivel español, solamente bastan dos hechos recientes que nos deben poner bajo alerta. El fraude a la Empresa Municipal de Transporte EMT de Valencia (3), de 4 millones de euros durante septiembre de 2019 y la detención por parte de la Guardia Civil (4) en la operación Lavanco de tres residentes en España por estafar mediante el fraude del CEO un total de 10 millones de euros a 12 empresas en diez países extranjeros.

Lo más llamativo de esta estafa es que va dirigida a empresas de todo tipo y sector. Además, los empleados que caen en el fraude pueden ser grandes profesionales en su puesto, concienciados y despiertos, pero el arte de engañar de los cibercriminales es superior.

La acción de los *cibermalos* se centra en estafar a empleados para que realicen pagos fraudulentos a una tercera parte no autorizada, pensando que quien se lo ordena con urgencia y confidencialidad es uno de sus superiores jerárquicos, al que han suplantado previamente.

tribuna

En una primera fase, los cibercriminales estudian a fondo la empresa y a sus directivos, como el CEO o el CFO, hasta obtener cuentas de correo electrónico válidas y otros importantes datos de la organización. Explotan la inmensa información personal y empresarial que todos dejamos en las redes sociales -Ingeniería Social-.

En la segunda fase, utilizando la información conseguida se envían correos electrónicos falsos con instrucciones para realizar transferencias o envío de información confidencial a cuentas fraudulentas.

En la tercera fase, para que el empleado ejecute la transacción a la cuenta de los ciberdelincuentes, utilizan técnicas de presión por urgencia, confidencialidad, simulando confianza entre emisor y remitente. Una vez realizada la transferencia, hacen desaparecer dicho dinero inmediatamente.

Este procedimiento de actuación tiene múltiples variantes, pero lo importante es conocer y concienciar a todos los empleados sobre la existencia de esta estafa y cómo prevenirla y detectarla. Una de las mejores maneras de protegerse dentro de una organización es, por tanto, poner en marcha planes de concienciación o persuasión, basados principalmente en:

- Sospechar siempre de correos con asuntos muy utilizados por este tipo de fraude, como *Important, Confidential o Notification of payment received*.
- Observar muy bien las direcciones origen de los correos sospechosos.
- Implantar procedimientos de doble verificación en la empresa entre personas y sistemas de doble factor de autenticación.
- Utilizar sistemas de gestión de la identidad y de firma electrónica para autenticación fuerte de los usuarios.
- Realizar planes de concienciación y persuasión continuos en la organización.
- Disponer de servicios avanzados de prevención y detección temprana.
- Diseñar y entrenar procedimientos de respuesta ante incidentes y planes de resiliencia.

El futuro que nos espera con el fraude del CEO es complejo y peligroso. El mal ha existido siempre y existirá. El *cibermal* además está potenciado por una sociedad global con un ritmo frenético. Sin embargo, el conocimiento, la formación e información puede ser nuestro salvavidas. La persona, que es el eslabón más débil de la ciberseguridad, es, a su vez, la defensa más fuerte contra los ciberataques que nos depara el futuro. Personas con principios y empresas especializadas en este ámbito, siempre estaremos aquí para defender a nuestra sociedad, adaptándonos al ritmo de los tiempos.