

## Desayunos ASTIC

# Soluciones de movilidad y seguridad para el sector público

**POR MAOLE CEREZO**  
REDACTORA JEFE DE BOLETIC

**FOTOS** AITOR DIAGO

Evento patrocinado por



EMC enfocó su participación reflexionando sobre qué es lo que puede aportar la seguridad a la movilidad. Javier Bustillo, Director de AAPP de la compañía inició su intervención recordando que su división de seguridad proviene de la adquisición de una de las compañías punteras en este sector RSA conocida, como apuntó el directivo “por sus tokens”. Entre sus servicios, ofrecen soluciones de garantía de identidad y de control de acceso, cifrado y gestión de claves, cumplimiento y seguridad de gestión de la información y la protección contra fraudes. Bustillo propuso atacar el tema de debate desde dos escenarios de actualidad en la AAPP “el teletrabajo y la conciliación de la vida familiar, y el portal del ciudadano, en los que los riesgos son comunes y el principal es el robo de la identidad”.

Manuel Lorenzo, responsable de la división de seguridad de EMC2 compartió con los presentes las experiencias que la compañía tiene en varios organismos de la administración, como puede ser la Agencia Tributaria o el Ministerio del Exterior. Puso en común evidencias compartidas por todos los presentes, como que “cuando uno trabaja remotamente, la barrera de la autenticación se pierde y, por ello, lo que hay que reforzar son los métodos de autenticación, para tener la certeza de que la persona que está entrando sea quien dice ser”. En el caso del portal del ciudadano

Los desayunos de ASTIC se han convertido en un clásico en el que sus miembros participan muy activamente y, este año, se están incorporando compañeros de las últimas promociones. Además de tratar en profundidad los temas propuestos en estos encuentros, socios y colaboradores de las empresas patrocinadores comparten experiencias profesionales. El pasado 27 de enero tuvo lugar el encuentro “ Soluciones de movilidad y seguridad para el sector público”, en el que participaron más de 25 personas. Francisco Antón, Presidente de ASTIC, lo inauguró y presentó a los ponentes de las empresas patrocinadores, EMC2, Microsoft y Siemens.

“esto no es trivial, los portales abren una puerta, no sólo a que alguien se haga pasar por otra persona, sino que incluso se haga pasar por nuestro portal del ciudadano para conseguir datos personales de nuestros ciudadanos, para la creación de páginas de phishing...”

¿Cómo abordó EMC2 este problema en la Agencia Tributaria? Aplicando “herramientas con las que históricamente hemos trabajado en bancos, sanidad... clientes de RSA. Los mismos sistemas estadísticos que empleamos para las entidades financieras, con motor de riesgo, son los que empleamos en la Administración Pública, una tecnología testada”.

Lorenzo hace reparar en que, “como entidad pública, es esencial cuidar la imagen de nuestros portales, y por ende, la nuestra” y en que cómo autenticar al ciudadano es un tema “controvertido”. El DNI digital es una de las alternativas iniciales para ello, pero “también tiene sus problemas, hay temas que no se han resuelto”. Por ello, señala “es interesante que ese tipo de acceso cuente con una plataforma que acepte todos los certificados que en la actualidad hay en el mercado, a la vez que sean más robustos”. En el caso de los empleados “podemos tener más control sobre ellos, si podemos pedir ciertas condiciones para entrar, aplicar el uso del token tradicional de RSA –disponibles también para »



**Más de 25 personas se reunieron en el desayuno organizado por ASTIC que contó con el patrocinio de EMC, Microsoft y Siemens**

dispositivos móviles que está ganando gran popularidad y facilitando el acceso remoto– o bien poner motores de riesgo” pero esto último “aún no lo hacemos en España”.

Maureen Manubens, Jefe de producto de CRM Microsoft Dynamics, una solución de gestión de relaciones, que va más allá de la tradicional de gestión de ventas, marketing servicios, “para gestionar relaciones con el ciudadano” comenzó apuntando que “en el entorno de empresa pública, uno de nuestros puntos fuertes es que, con independencia de que un ciudadano acceda a un portal, por detrás nosotros tenemos una manera estructurada de gestionar una serie de procesos y actividades, y esto en cuatro escenarios distintos”. Los escenarios a los que se refiere Manubens son: en el área de gobierno, “todo lo referido a la gestión de comunicación hacia los ciudadanos; la recepción y tramitación estructurada –con unos flujos de trabajo por detrás– de incidencias del ciudadano; campañas de comunicación...” Un segundo, en el que la compañía tiene amplia presencia, es “el referido a la gestión y comunicación del

ciudadano con dependencia, y la comunicación y gestión automatizada de campañas de desempleo”. Un tercer escenario es el relacionado con “la gestión de relaciones, empleado como CAU interno, de cualquier tipo de departamento de informática de una entidad para tramitar las incidencias de sus empleados y generar un flujo de trabajo para que esas incidencias se gestionen”. El cuarto escenario se enmarca en “entidades u organismos semi-públicos, cámaras de comercio, asociaciones”. Y “para estos cuatro escenarios aportamos un software que permite el acceso desde cualquier dispositivo”. Porque, “una de las cosas de las que nos sentimos orgullosos es de la completa integración que tenemos con todas las soluciones y herramientas de Microsoft”.

Antes de presentar al ponente de Qurius, empresa partner de Microsoft, la Jefa de Producto, explicaba cómo “en el área de dynamics trabajamos con partners implantadores, y Qurius es líder en el área de dynamics, y en concreto en CRM. Participan en el testing de todas las versiones que

»

vamos a sacar de dynamics CRM en euskera, gallego y catalán”.

Cabe recordar que EMC y Microsoft Corporation ampliaron su alianza estratégica para mejorar la protección de su información sensible y para que puedan compartirla de la manera más segura. Ambas compañías trabajan en una propuesta que ayuda a proteger la información en toda la infraestructura basada en contenido, contexto e identidad

### Casos de éxito

Javier Garagorri, especialista en solución CRM de Qurius dio algunas pinceladas de varios casos de éxito de la compañía. Antes, a modo de preámbulo, planteó un escenario en el que “tenemos nuestro interlocutor, nuestro ciudadano, que cada vez se dirige a nosotros de distintos modos. Todos ellos han de estar procedimentados dentro de la organización, de modo que dentro de una estrategia dirigida con dynamic CRM, nos proporcione una imagen clara del ciudadano o interlocutor para explotar, mediante reglas claras, que es lo que queremos hacer con él”. Dynamics CRM nos permita “lanzarle comunicaciones y ser capaces de llegar utilizando CRM de manera móvil. Independizamos la gestión del medio, de esta manera, lo que buscamos es potenciar a nuestro interlocutor”.

En el Ministerio de educación “hemos realizado una integración Web para que todo el público externo pueda suscribirse a alertas para becas, y tenemos la capacidad de hacer el seguimiento y comunicarnos con los ciudadanos, de la manera que ellos nos han solicitado, una vez resueltas esas becas. Capturamos la información en portales, para devolverlas según las preferencias del usuario del servicio”. En la Cámara de Comercio de Guipúzcoa, “nos encargamos del mantenimiento de todo su directorio empresarial. Tenemos, en un repositorio, todas las actividades de interés de todas las empresas de Guipúzcoa para gestionar con ellas comunicaciones, eventos... etc. Ello, con el fin, de implicar al tejido empresarial dentro de la Cámara”.

En el metro de Madrid, “recogemos las incidencias reportadas por todos los trabajadores que reciben soporte del departamento de IT y le damos un enrutamiento con reglas de negocio pre-configuradas dentro del CRM, para poder cumplir con las expectativas de calidad, tanto del usuario final del servicio, como del propio departamento de gestión de incidencias. En el Ministerio de Economía, »



**Alicia Álvarez**



**Blas Cordero**



**Borja Prieto**



**Carlos Ariza de Siemens**



**Carlos Maza**



**Carmen Cavanillas**



**Carmen García**



**Celia Tenés**



**Ernesto Garrote**



**Fernando García**



**Fernando Martín**



**Francisco Antón**



**Iván Ledesma**



**Javier de Andrés**



**Javier Garagorri de Microsoft-Qurius**



**Javier Losana de Siemens**

»

“considerando al usuario interno como nuestro, hemos desplegado la clave pública de infraestructura, llevado CRM hasta el funcionario recogiendo sus datos, entregándole su infraestructura de seguridad y volviendo con ella para hacer una trazabilidad, un control, un seguimiento de todos. Y, al mismo tiempo, hacer un despliegue rápido de encuestas. Queríamos tener un retorno rápido y hacer una trazabilidad de cuándo respondió el usuario, que respondió, si empezó la encuesta y no la terminó, si ha pasado un tiempo estimado de respuesta para que la terminase, tiempo desde que la empezó y la terminó...”

En Red. es “estamos dando un canal al ciudadano para que acceda a un servicio de información vía telefónica electrónica, con unas reglas de respuestas que le tenemos que ofrecer con una base de datos de conocimiento y una gestión y monitorización de todas las incidencias y un control, tanto de tiempo, como de resultados de ese call center que está atendiendo a las llamadas”. Garagorri concluye su intervención haciendo hincapié en que “CRM Microsoft Dynamics no es sólo una herramienta per sé sino que, además, está perfectamente integrada con su entorno y permite capturar información útil para tener una imagen global de nuestros interlocutores”.

Javier Losana, Responsable de Comunicaciones Unificadas para el Sur de Europa de Siemens Enterprise Communications compartió con los presentes la interpretación que su compañía hace del concepto de movilidad: “en principio, está claro que movilidad es ofrecer a nuestros trabajadores en el ámbito de las tecnologías de la información la posibilidad de trabajar en cualquier lugar, trabajadores que están empleando medios de comunicación y un ordenador”. Para ello, propone varias opciones, recordando antes que “se podría ofrecer movilidad absoluta a nuestros empleados con un teléfono y una conexión de datos para el ordenador, pero los costes serían inabordables”.

¿Qué soluciones hay? Una amplia variedad de ellas –según éste– y, su sugerencia “no es dar una solución única, sino definir las necesidades de cada uno de los empleados y dar soluciones de acuerdo a éstas. La aproximación más ventajosa es la que se va tratando por colectivos y dándoles respuesta, implantándolas con el menor coste posible y con el máximo impacto para los usuarios”. Losana propone tres alternativas. La primera sería “el trabajador de movilidad en el entorno campus, ubicaciones de Administración Pública que tienen

múltiples edificios. Para dar una cobertura máxima es complicado, siempre habrá islas. En estos emplazamientos proponemos una opción, que ya está madura, la convergencia fija móvil. Empleamos tecnología corporativa cuando nos encontramos en el ámbito de cobertura wifi, y cuando nos quedamos sin cobertura conectamos con la red gsm. Al volver nuevamente a un lugar con cobertura wifi se interrumpe la llamada vía gsm y se mantiene la llamada interna sin generar costes de conexión. Hay también soluciones de reentrada, dejamos de pagar la telefonía móvil en cuanto entramos en una zona de cobertura wifi”.

No obstante, a medida que se va experimentando con estas soluciones se encuentran algunas dificultades asociadas a un entorno de telefonía profesional. Por ejemplo, una de ellas es el agotamiento de la batería “un profesional necesita conectividad durante ocho horas habitualmente como mínimo. Y en los teléfonos comerciales empezamos a tener problemas de comunicación a las cuatro o cinco horas de su uso. Para salvar esta situación, nos podemos apoyar en otra solución el *one number service* que nos permite mantener nuestro número telefónico al cambiar de terminal, incluso con un teléfono que nos prestan. Ese cambio de terminal telefónico lo podríamos hacer desde nuestro propio ordenador, desde un cliente Web con la aplicación de *one number service*, un cliente móvil o incluso a través de un portal de voz”.

La segunda alternativa que propone el directivo da respuesta al teletrabajador. El funcionario puede realizar su trabajo “desde la oficina u otro lugar”. El teletrabajo “va a ser una prioridad cada vez mayor, y hay ya soluciones que nos permiten experimentar con pilotos, a la escala que queramos”. ¿Cómo ofrecer a un trabajador de las TI un puesto de trabajo en su casa? “Mediante el CEP, *Communications Everest Procces*, una propuesta que permite incrustar comunicaciones en las aplicaciones en las que nuestros usuarios están trabajando, seleccionando que funciones de colaboración queremos incrustar. En un portal web de SAP, donde podemos llegar a través de una línea de datos de alta o baja velocidad, incrustamos las funciones de comunicación”.

Tercer escenario que presenta Siemens para ofrecer soluciones es el del perfil directivo. Para éste, la compañía da “la posibilidad de tener un control sobre sus comunicaciones”. Entre las prestaciones “configurar audio conferencias; dar acceso a los contactos que se desee; decidir que se quiere que ocurra con el resto de llamadas. Mediante un cliente web, la secretaria del »



**José Antonio García**



**José Luis San Martín**



**Juan Fernando Muñoz**



**Leonor Torres**



**Luis de Eusebio**



**Mª Jesús Llorente de Microsoft-Qurius**



**Mariano Pino de Microsoft**



**Manuel Lorenzo de EMC**

directivo puede alimentar la lista de números a los que se le permite el acceso”. A la vez, “con *one number service* se tiene la posibilidad de cambiar de terminal. Las prestaciones no son las mismas que las del teléfono fijo, pero son muchas en movilidad”. Se está generando ya una integración de cliente de comunicaciones unificadas con el cliente de convergencia fijo móvil. “Generar conferencias *ad hoc*, seleccionar una serie de personas y llamarlas desde el móvil, modificar tu dispositivo preferido con un clic, llevarse desde un fijo al móvil la llamada solo a golpe de clic... todo esto ya va a ser una realidad comercial. La integración de ambos mundos en un mismo dispositivo es lo que nos va a aportar las comunicaciones unificadas”.

### “Nos preocupa”

Luis de Eusebio plantea a EMC2 tres cuestiones que “nos preocupan” con el fin de conocer las soluciones de la compañía para la AAPP. La primera es “la implementación de las sedes electrónicas, una segunda el archivo y custodia de la documentación digital y la tercera las tarjetas de los empleados”. La solución que, tal y como explica Javier Bustillo, la compañía tiene para el archivo y custodia se llama Centera. “Un sistema de almacenamiento que no tiene nada que ver con los sistemas tradicionales. El almacenamiento se realiza a través de una API, directamente desde la aplicación, y está físicamente conectado con la red por al menos dos nodos de acceso en Centera. Si la aplicación no está conectada directamente, el sistema Legato DiskXtender para EMC Centera ofrece una forma de migrar información a Centera. Esta solución ofrece una ventaja significativa para aquellos sectores que gestionan grandes volúmenes de datos y que necesitan tenerlos disponibles durante muchos años”. Está muy implantada en la administración, con más de cincuenta referencias, entre ellas figuran en la AGE, “el Ministerio de Agricultura, Fomento, Educación Política Social y Deporte, el Ministerio de Defensa o el de Interior”. En la administración regional EMC2 cuenta con experiencias relevantes como “la custodia del archivo de Simancas; en la Consejería de Ordenación Territorial de Valladolid se utiliza para salvaguardar custodia firmada durante más de 50 años, también se emplea en el Catastro... Utilizan este tipo de repositorios, que no son transaccionales, pero sí *on-line*. Permite recuperar la información *on-line* independientemente de la aplicación desde la que se acceda y con una característica esencial: su direccionamiento está basado en su propio contenido. De tal manera que, lo que se genera para guardar la información, es una huella digital del contenido y esto es lo que se certifica”.

Manuel Lorenzo añade que “en el tema de control de datos sensibles, EMC cuenta con una plataforma *enterprise* de gestión de claves que es *key manager*, que permite que una clave sea controlada desde un único punto central donde es generada y custodiada. Si un documento tiene que estar cifrado y necesita control de acceso para poder leerlo, este control tiene que estar centralizado”. Porque, prosigue Lorenzo, “algo muy importante cuando hablamos de datos sensibles es ¿como evito la fuga de éstos? Lo que llamamos el *data lost prevention* es uno de los puntos fuertes de RSA, que intenta prevenir que los datos sensibles estén controlados, no haya fugas”. Respondiendo a la cuestión sobre la tarjeta de empleados, el portavoz de RSA explica como “proporcionamos toda la parte de control de acceso a las aplicaciones de forma unificada y toda la de gestión completa de la PKI, (Infraestructura de Clave Pública).

La compañía también ofrece soluciones que garantizan la identidad de las partes implicadas en la implementación de la sede electrónica. Lorenzo se refiere a varias propuestas: “disponemos de varias soluciones de identificación del *site to user* para que la sede con la que se conecte el usuario se autentique contra él, esté seguro de que habla con quien tiene que hacerlo”. ¿Qué métodos hay de relación a largo plazo? “Métodos que se emplean en banca, pero que en la AAPP son difíciles de aplicar, ya que la relación a largo plazo aún la tenemos que crear. A medida que avancemos con la relación con el ciudadano podremos implantar este tipo de soluciones. La autenticación del ciudadano a la entidad si que lo hemos implantado ya”.

Por su parte, Microsoft propone su CRM que, tal y como explica Maureen Manubens “posibilita tener un *back office*, una estructura muy fácil de usar y desplegar, que no tiene prácticamente una curva de aprendizaje para poder generar ese tipo de relaciones más duraderas con los ciudadanos y, en base a esto, estructurar una autenticación de site a éste, poder desplegar pkis, etc.”

Otra cuestión que Luis de Eusebio saca a la palestra es la inquietud que existe entre los compañeros sobre “en qué formatos hay que guardar estos documentos a 50 años vista”. Bustillo, explica como en EMC “guardamos y no identificamos el formato, porque nosotros salvaguardamos y custodiamos de manera certificada con ceros y unos, los responsables de acceder a interpretar la información son los dueños de las aplicaciones. Con CENTERA, somos compatibles con más de mil aplicaciones para guardar, de manera certificada, documentación, información en formato electrónico”. Pero “lo que si hacemos es firmar acuerdos de custodia y salvaguarda a cincuenta años. Pone como »

ejemplo de ello el rubricado con “la Biblioteca John Fitzgerald Kennedy”. Porque para “salvaguardar información, en este caso histórica, la administración necesita el compromiso del fabricante para que le asegure que, el portador físico y lógico donde la empresa salvaguarde y custodie toda la información, la haga compatible dentro de 50 años”.

La apuesta de Microsoft es “ir a estándares y separar en nuestros aplicativos tradicionales el formato de los datos en su almacenamiento de las propias aplicaciones, para que no haya una dependencia entre la aplicación y el dato que se almacena de cara a su pervivencia en el tiempo.

Francisco Antón plantea a EMC cómo abordar la certificación de una plataforma segura, por ejemplo cuando la agencia tributaria pone su sello de certificación. Para el director de AAPP de la compañía “el certificado no es más que una lista de ceros y unos. Existe una aplicación, por encima, que es el organismo certificador con su aplicación, sea cualquiera de las 16 entidades certificadoras de España. Éstas son las responsables de mantener la compatibilidad de los certificados en el tiempo. Nosotros certificamos que, ese dato salvaguardado y custodiado, va a estar disponible de aquí a 50 años. Si la entidad certificadora es compatible con su propio formato en el tiempo, sus datos van a tenerlos salvaguardados y, de manera legal, vamos a certificar que si ha habido alguna modificación va a quedar registrado”.

¿Y cómo se lleva a cabo la autenticación del ciudadano en relaciones puntuales con la Administración? Este es, según José Luis San Martín, el principal problema que tienen las Administraciones Públicas. Porque, “los patrones estadísticos para relaciones a largo plazo tienen sentido, pero para llegar a una masa grande de población, lo único que veo con sentido son los elementos biométricos”. Pero “no encuentro ninguna propuesta en este sentido, y el principal problema se nos plantea, cuando es el ciudadano quien inicia la relación” ¿Cual es la experiencia de EMC? También Carlos Maza incide en este punto y plantea si ¿existe alguna tecnología para poner en 2009 servicios que requieran la identificación de la persona que está al otro lado de la línea, bien sea en un fijo o en un móvil y, en su caso, la firma?

Mariano Pino, Director de Administración Central de Microsoft coincide con la dificultad que entraña la autenticación en relaciones puntuales, porque a más a más, “se crea más incertidumbre y se requieren más comprobaciones que con las relaciones a largo plazo. »



**Maureen Manubens de Microsoft**



**Miguel Ángel Rodríguez**



**Pablo Burgos**



**Rocío Montalbán**



**Ventura Alcaide de Siemens**

En nuestra experiencia, los datos biométricos no son la solución. Nosotros creamos patrones de comportamiento en los grupos. En donde nuestra compañía está trabajando más es en la identificación en las llamadas telefónicas, hacemos preguntas aleatorias al usuario que nos sirven para asegurarnos que la persona con la que hablamos es quien dice ser. Pero esta vía plantea aún complicaciones en España porque no se dispone de la información necesaria para ello, no disponemos de los datos privados que nos permitan la autenticación. En EEUU están más avanzados, tienen un sistema de almacenamiento de datos que recoge información privada del ciudadano". De momento, en España, en lo que se refiere a la gestión de portales, "nosotros estamos apostando por el DNI digital, no estamos yendo más allá". Es importante señalar, comenta Maureen Manubens, que "la tecnología va paralela a la realidad de nuestros clientes. Y se da la circunstancia de que, el propio cliente, no tiene certeza de la información de sus usuarios lo que conlleva, a su vez, la imposibilidad de autenticación por nuestra parte".

Ante esta propuesta, Celia Tenés puntualiza que con la ley de Protección de datos resulta complicado recopilar ciertas informaciones privadas para usarlas en la administración. Mientras que Alicia Álvarez, comparte con los presentes su satisfacción por "el paso histórico que se dió en el Ministerio de Interior al cambiar sus sistemas de almacenamientos por Centera". Fue decisivo para ello, como explicó la directiva, el informe jurídico de EMC que se presentó a los jueces, en el que se garantizaban los datos sensibles que se manejan en este Ministerio como son las escuchas telefónicas.

### La banda ancha, tema pendiente

Alicia Álvarez también comenta cómo en el Ministerio del Interior se dispone de "una de las redes más importantes del mundo TETRAPOL", pero "tenemos problemas para poner al usuario final aplicaciones de banda ancha. Nuestra policía tiene que llevar un móvil y un terminal TETRAPOL y queremos terminar con esta situación y que empleen biométrico para la identificación, pero para ello necesitamos banda ancha. ". Nuestras aplicaciones para policía, guardia y fuerzas de seguridad del estado se ven paradas porque no hay interoperabilidad entre redes de emergencia y telefonía".

También la policía del Ayuntamiento de Madrid necesita banda ancha para disfrutar de una verdadera "oficina en la calle", tal y como señala Fernando García, que explica como "los agentes trabajan con una PDA y un portátil, no

tienen nada integrado, los datos van por un lado y la voz por otra, y cuando hay catástrofes, los sistemas de movilidad de teléfono se colapsan". Pero, ¿cómo tener sistemas de transmisión de datos en movilidad con una garantía de servicio de que no se sature la red? Según el directivo, a día de hoy, nadie responde a esta pregunta. Y otra cuestión que lanza es ¿Cómo guardamos los datos?

García comparte con los presentes una experiencia vivida cuando trabajaba en la Intervención General del Estado, en la que el papel "nos salvó. Necesitábamos recuperar unos expedientes de cuentas, teníamos las cintas, podíamos leer los ceros y los unos, pero no teníamos el ordenador apropiado, que hacía años que ya no se fabricaba. No fuimos capaces de recuperar la información que nos reclamó el juez, y salvamos la situación gracias al papel". Prosigue haciendo una reflexión en voz alta "ahora que estamos haciendo desaparecer el papel en la AAPP y lo guardamos en formato digital, habrá algún sistema de base de datos alternativo a la información impresa? Podemos tener un CENTERA, pero si no podemos leerlo transcurridos x años...".

Para terminar su intervención, García plantea: "¿que soluciones globales ofrecen de *single signe on*? En nuestras organizaciones tenemos firma electrónica, acceso... a la vez que empleamos diez contraseñas diferentes, tenemos una gran seguridad, pero con x claves de accesos, al final terminamos apuntándolas en papel. ¿Cómo aunar simplificación y seguridad?, porque, en cuanto tengo tres contraseñas diferentes, las escribes en un *post it* que se guarda en los cajones"

Siemens responde a ello recordando que "nuestro *token* de toda la vida es una *password* única. Pero es un hecho que uno de los problemas es el *single signe on*". Porque, la realidad es que "no es un proceso sencillo poner de acuerdo a distintos ministerios para permitir que una persona salte de un web de un organismo a otro con un único *password*". Ya que de lo que se trata no es "de un problema tecnológico, sino de ponerse de acuerdo internamente". En opinión de Francisco Antón, "un *token* universal no existe". 🍷