"No hay en Europa un centro de investigación en seguridad digital como el que tenemos en Pamplona. Eso es algo que debemos aprovechar todos"

Entrevista a
Xabier Mitxelena Ruiz
Director General S21sec

ENTREVISTA REALIZADA POR
Jesús Rivero
PRESIDENTE DE DINTEL
Y EDITOR DE LA REVISTA a+

FOTOS
Javier Fuentes

El 2000, se asoció en los alrededores de aquellos años, con su famoso <<efecto>>. Mucho ruido y pocas nueces, que el tiempo nos ha ido haciendo olvidar. Aunque sin tanta repercusión mediática, aquel año 2000, sí que generó <<muchas nueces>> –que ahora se están recogiendo en el sector de la seguridad– y, sin apenas ruido, entonces: fue el año en que se fundó ***S21sec****, empresa de la que* ***Xabier Mitxelena*** *es Director General, además de <<fundador>>.*

Con formación académica de Ingeniero de Organización, y MBA en Dirección Comercial y Marketing, por la Universidad de Deusto, ***Xabier Mitxelena****, ha sabido apoyarse a la perfección en su actividad profesional, en ambos pilares: el técnico (a nivel organizativo) y el comercial (en su vertiente de marketing).*

Pero por encima de todo ello, ***Xabier*** *es un emprendedor, según demostró con anterioridad, cuando fundó* ***ATE Internet*** *y* ***ATE Consultoría****; previamente había sido Gerente de* ***ATE Informática****. Es en aquella época, cuando se consolida su experiencia profesional, no sólo en el sector informático puro, sino también en los asuntos de calidad y seguridad informática; por supuesto, su experiencia está fundamentada, en el origen, por su etapa inicial de consultor en BULL y SAYMA.*

Ahora bien, cuando hablas con el Ingeniero Mitxelena, no sólo trasciende la solidez de su formación técnica, con una impecable precisión terminológica y una clarividente visión globalizadora y de prospección tecnológica futurista.

Efectivamente, lo que me impacta positivamente de ***Xabier*** *es, su seguridad personal y su brillantez expositiva, con absoluta capacidad de convicción.*

Es en el 2009, cuando ***S2sec*** *ha empezado a implicarse más en las actividades de* ***DINTEL****. Pues bien, sin menospreciar la ayuda económica de su "patrocinio global 2009", ahora que no nos escucha nadie, puedo asegurarle amigo lector, que la mayor contribución que nos ha dado y nos dará* ***S21sec****, es la oportunidad de colaborar con un líder tecnológico del nivel y proyección internacional de esta compañía española volcada en la I+D.*

Xabier*, encantado de poder reconocer nuestro enriquecimiento derivado de vuestra actual colaboración y, muchas gracias por el tiempo concedido para esta entrevista.*

Para empezar, y aunque me lo has explicado en varias ocasiones, con anécdota incluida, pensando en nuestros lectores, ¿podrías darnos la "definición" de S21sec como nombre de empresa?

La palabra **S21sec** procede de cuando pusimos en marcha nuestro proyecto empresarial orientado a la especialización en seguridad. Queríamos un proyecto con una continuidad en el tiempo. La idea surgió en 1999 -o sea siglo XX- y teníamos claro que la seguridad no era solamente poner barreras, *firewalls*, etc. Buscábamos una palabra que permitiera definir un modelo de empresa con continuidad en el tiempo. Los dos conceptos claros eran, por tanto, la palabra "Seguridad" por un lado y por otro el futuro que en ese momento era el "siglo 21"; por lo que S21sec es un concepto *"spanglish"* que viene a significar **"Siglo 21 security"**: *la seguridad del siglo 21*.

La anécdota sucedió en Sevilla, en una reunión donde estaban sevillanos y americanos y quise adelantarme a que me preguntasen sobre el significado de S21sec, diciendo que era *"Sentury"* 21 security.

Por otra parte, y ya más formalmente, ¿cuál es su misión?, ¿cuáles son sus objetivos a corto, medio y largo plazo, tomando como referencia abril 2009?

La misión de la compañía es una consecuencia de su propio desarrollo, y puede resumirse diciendo que es la gestión y prevención de los riesgos en la vida digital para las organizaciones y las personas. Entendemos que en la sociedad actual, con el impacto de Internet y de los sistemas de información, la sociedad se ha transformado y estamos todos en un

modelo digital en el cual es común intercambiar datos y conceptos económicos, establecer relaciones Administración-Ciudadano, Administración-Empresa y Empresa-Ciudadano.

¿Por qué decimos gestión? Pues porque entendemos que la seguridad total no existe y los riesgos son conceptos dinámicos que deben estar vigilados continuamente en cualquier tipo de organización. Y la parte preventiva es un objetivo, es decir, siempre que seamos capaces de generar metodologías y servicios que permitan prevenir se estará trabajando el modelo de seguridad con éxito.

Con respecto a los objetivos a corto/medio/largo plazo es una pregunta difícil ya que en abril de 2009 estamos inmersos en un período de incertidumbre económica global. En todo caso, en nuestra visión de la compañía los objetivos siempre han sido dos: ser un referente a nivel mundial en el entorno de la innovación en materia de seguridad y ser líderes en materia de servicios de seguridad en aquellos mercados en los que estemos operando. En el corto/medio/largo plazo nuestros objetivos siempre van en esa línea.

Somos una compañía que basa su diferenciación en la innovación, en el I+D+i, intentando mejorar procesos y tecnologías para ofrecer el mejor servicio. Esto requiere de un esfuerzo de inversión ímprobo y **S21sec** invierte un 25% de los recursos propios en este concepto. Desde el punto de vista de los accionistas, esto hace que la compañía se vea como un proyecto en el tiempo de generación de valor y de liderazgo. También deseamos hacer ver que en España se tiene capacidad de innovación y de generar tecnología tan buena como la que viene de fuera, y con la virtud de ser más creativos e, inclusive, más intuitivos. En el mundo de oportunidades que supone Internet queremos aportar el valor de la confianza.

En su accionariado están presentes, actualmente, dos fondos de Capital Riesgo. ¿Qué se pretende conseguir con su participación en el accionariado, máxime cuando tenéis a gala no repartir dividendos? ¿Tiene esa participación establecido un plazo temporal? ¿Pueden llegar a ser mayoritarios?

Además de lo que acabamos de comentar, uno de los objetivos fundamentales de una compañía como **S21sec** es ganar dinero ya que una compañía que no gana dinero no tiene futuro. En nuestro caso, no repartir dividendos simplemente es un concepto vocacional que nos hace reinvertir los beneficios directamente en la compañía para obtener un punto de madurez que permita un buen apalancamiento.

Desde el punto de vista de los fondos que están trabajando en la compañía, daría una característica: no son fondos que buscan el beneficio anual puro y duro sino que son fondos asociados a lo que es peculiar de la compañía y su objetivo fundamental es acompañarnos en el tiempo para salir de la compañía con un beneficio asociado a la generación de valor.

Los accionistas que han estado en la compañía, la han abandonado porque han cumplido su momento estratégico obteniendo por ello una plusvalía interesante y han quedado satisfechos. Siempre se ha obtenido el compromiso por parte de los accionistas de aceptar que nuestro modelo de desarrollo está basado en obtener el liderazgo y es diferente a los modelos americanos de crecimiento y beneficio rápidos.

Por parte de los fondos accionistas existe un compromiso de permanencia en el tiempo para ayudar al Equipo de Dirección a generar un modelo de gestión adecuado al desarrollo de la compañía. El concepto "tiempo" lo marca la madurez de la compañía y cuando se alcanza un estatus determinado es cuando en el Consejo de Administración se toma la decisión de dar pasos adelante para dejar paso a nuevos inversores.

En **S21sec** no existen mayorías que puedan "dominar" la gestión de la compañía sino que existen un conjunto de minorías lo suficientemente complementarias como para poder llevar una gestión adecuada de la misma. Hasta ahora

todas las decisiones se han tomado por consenso y sobre todo por convencimiento.

¿Está prevista una ampliación de la colaboración con Verisign?

La vocación de **S21sec** es ser una compañía española conceptual y accionarialmente. Dicho esto, con respecto a Verisign hay que decir que colaborar con ellos ha sido un acierto en el camino trazado, sobre todo porque en el mundo de la seguridad nadie tiene el 100% de la información y del conocimiento. Es sabido que Verisign es una compañía líder mundial en seguridad que cotiza en el Nasdaq. La colaboración con ellos nos ha permitido tener un centro de gestión 24x7 para nuestros clientes y sobre todo ha permitido el intercambio de información. La seguridad se basa en el conocimiento y cuanto más se sabe sobre un concepto tecnológico, antes se pueden tomar decisiones. Verisign nos ha aportado "inteligencia" y eso ha permitido dar un valor añadido a nuestros clientes. Hace cuatro años, cuando empezamos a trabajar en la prevención del fraude la tecnología era en más de un 75% de Verisign; en la actualidad, el 99% de la metodología que utilizamos es nuestra porque somos capaces de aprender y de innovar. La colaboración con Verisign es interesante por la información y la "inteligencia" que aporta pero dentro de la estrategia de la compañía no se contempla el crecimiento de la participación de Verisign en **S21sec** y tampoco creo que ellos deseen otra cosa.

¿Cuál es la filosofía y el planteamiento conceptual que hace S21sec de la seguridad? ¿Cómo aplican la inteligencia a sus servicios de seguridad?

La seguridad no es un producto sino un proceso dinámico, que está ligado a cada uno de los componentes que dan lugar a una solución. La seguridad no se basa en la foto de un día sino que es un proceso dinámico. Entendemos que todo aquello en lo que estamos trabajando nos permite obtener la suficiente información como para poder aplicarlo a un modelo de servicios. Creemos que la tecnología es un medio y es un concepto que debemos tener en todos los sistemas de información y no sólo en el modelo de seguridad. El objetivo perseguido es ayudar a nuestros clientes a que hagan mejor sus negocios siendo nosotros sus socios de seguridad.

Para nosotros el concepto de inteligencia es el de información. Con un dato se pueden tomar un conjunto de decisiones y con muchos datos se pueden tomar muchas más decisiones, es decir, cuanta más información se tiene sobre lo que puede ser un problema de seguridad, más facilidad se tiene para poder actuar de una manera determinada. La realidad ha demostrado que está muy bien comprar productos de seguridad pero es absolutamente necesario interpretar qué es lo que está pasando en tus sistemas para tomar las decisiones adecuadas. La seguridad no es un concepto estanco sino que son un conjunto de datos correlativos que permiten tomar decisiones.

Si hoy en día en el campo de la salud estamos investigando el ADN para tener suficiente información como para crear un entorno preventivo para las personas, en el entorno digital se ha bajado al concepto del LOG que es el último nivel de datos que existe. Cuanta más información se tenga a nivel de LOG de todos los elementos que forman parte de un modelo de negocio, más fácil será interpretar el concepto de riesgo.

Así es como se trabaja en **S21sec** en todos los ámbitos, creando tecnología que permita analizar la información para poder prevenir ciertos tipos de actos y sobre todo orientando la seguridad a un cuadro de mandos que permita medir en cada momento cuál es el nivel de riesgo de un cliente.

S21sec se siente orgullosa de la tecnología que desarrolla en su centro de I+D+i ¿En qué medida utilizan tecnología propia y en qué medida de otros en sus soluciones? ¿Cuántas personas de la plantilla de S21sec están asignadas a tareas de investigación, desarrollo e innovación? ¿Cuál es su inversión anual en I+D+i?

Cuando nace **S21sec** en el año 2000, lo hace con una vocación de innovar, investigar y generar tecnologías que permitan dar un valor diferente al cliente. Se pretendía cubrir huecos que no se habían tenido en cuenta y que había que empezar a considerar. Nos ha costado cinco o seis años convencer a un conjunto de accionistas de que esto se tenía que ordenar y centralizar para obtener un rendimiento final. Tener hoy en día un centro de I+D+i en Pamplona con más de 80 personas trabajando y que innova en todos los campos que dan valor a los procesos de negocio, investigando en el concepto de infraestructuras críticas, estudiando los elementos que atacan las redes, troyanos, malware, etc., nos aporta un valor final que se aplica a los clientes. Hoy no hay en Europa un centro de investigación en seguridad digital como el que tenemos en Pamplona. Eso es algo que debemos aprovechar todos y no sólo nosotros como empresa que transmite algo, sino los propios clientes que se deben poder "aprovechar" de los resultados de las investigaciones generadas desde **S21sec**.

En la práctica, cuando existe tecnología de terceros que es capaz de cubrir las necesidades en un ámbito de la seguridad lo que hay que hacer es aprovecharla. En cinco años hemos pasado de trabajar con un 80% con tecnología de terceros a trabajar con un 80% de tecnología propia. Se ha mejorado de manera importante en la capacidad de respuesta al cliente y se ha mejorado sobre todo en la capacidad de prevención.

Cuando empezamos se invertían más de un 40% de los recursos propios en I+D+i, ahora esa inversión es del orden del 25%. En todos estos años se han activado más de 15 millones de euros en tecnologías propias, es decir, se ha generado tecnología por valor de 15 M€, y eso se refleja directamente en lo implantado en los clientes.

Siempre que se habla de I+D+i se juntan dos áreas que son por un lado la investigación, con un cierto número de personas, y luego está la gente que innova. Nosotros tenemos un grupo de 90 personas en I+D+i pero las otras 180 personas, aportan conocimiento a la innovación en un porcentaje importante. Éste es uno de los activos fundamentales de la compañía.

Por poner una cifra, la inversión en I+D+i en el año 2009 rondará los 4 millones de euros.

Entre vuestros clientes están las Administraciones Públicas, las grandes corporaciones y también empresas de tamaño medio ¿Cómo enfocan los temas de seguridad en cada caso? ¿Existen diferencias significativas entre sus respectivas estrategias?

Sí hay diferencias, sobre todo porque el concepto de la seguridad es algo inmaduro y no está embebido en los procesos de las compañías. Por desgracia cada uno aborda la seguridad en función de sus requisitos y después en función de la sensibilidad existente en la alta dirección, sin ser esto proporcional ni lineal.

El sector financiero empezó a abordar los modelos de seguridad a finales de los años 90, entendiendo que era un sector que estaba transformando su modelo de negocio hacia el mundo electrónico y al abrir una puerta a dicho modelo de negocio también se abrió la puerta a nuevos riesgos. Este sector es el que más ha empujado los modelos de seguridad.

Las AAPP y las grandes corporaciones han tenido un comportamiento diferente y, nos guste o no, es cuando entran en juego leyes como la de Protección de Datos, es decir cuando entra en juego la regulación o normalización es cuando se produce la concienciación y quien invierte más en seguridad empieza a ver que no es un gasto sino una inversión que reporta un beneficio.

Si se habla de las grandes corporaciones, quien está invirtiendo en seguridad está teniendo una apuesta clara por lo que puede ser un concepto de globalización. Las grandes compañías españolas que han abordado sus procesos de internacionalización y que ven en la tecnología una ventaja, por temas regulatorios y sobre todo por temas

de relaciones con clientes hacen una apuesta clara por el concepto de la confianza.

Con respecto a las AAPP es verdad que toda parte legal les ha ido ayudando a invertir en seguridad pero ha costado algo más de lo que nos habría gustado a todos. Todos esperábamos que a principios del 2000 las AAPP fueran de verdad el motor y han sido probablemente las leyes las que han ayudado y ha sido en los últimos tres años cuando la Administración está haciendo un impulso importante por el concepto de la Administración Electrónica. La famosa Ley 11 ha impulsado el concepto de confianza, es decir, todo el mundo ve que a través de la relaciones con los ciudadanos se genera un camino que permite ahorrar tiempo y dar un servicio de valor añadido. El DNI electrónico nos va a ayudar a todos a entender que existe un conjunto de herramientas que nos permiten trabajar a través de medios electrónicos aunque el despliegue va a tardar aún varios años y las aplicaciones deben estandarizarse más. Pero en los últimos años la Administración Pública está haciendo un gran esfuerzo por abordar procesos de gestión de riesgos en los servicios a clientes y eso es hacer una apuesta importante por la seguridad como el elemento de confianza en esta relación.

¿Qué impacto está teniendo la actual crisis económica en los temas de seguridad? ¿Qué previsiones crees que tendrán en este año 2009?

La crisis afecta directamente sobre todo a los sectores en los que el concepto "recesión" hace que se paren como puede ser la construcción con su gran repercusión en el empleo. Sin embargo en aquellos sectores en los cuales la aplicación directa de productos y servicios nos permiten mejorar o garantizar los procesos las compañías van a sufrir un poco menos la crisis. La seguridad es un elemento indispensable y entendemos que Internet es un camino sin retorno con lo cual en un proceso de transformación de las compañías Internet sólo tiene ventajas. Las posibles desventajas, los riesgos, se mitigan con la inversión en seguridad y aquellas empresas que han invertido en seguridad hasta la fecha van a seguir haciéndolo porque tienen claro que es un activo para ellas.

La crisis se va a reflejar en las AAPP ya que tienen menos ingresos y si la seguridad no ha tenido un papel principal en sus planes, se va a ver afectada. El gran problema de la crisis es que el potencial de crecimiento del mercado de la seguridad va a crecer menos que en años anteriores.

Va a haber muchos actores del mercado tecnológico que verán su continuidad en la seguridad y eso va a hacer que este mercado sea más competitivo pero también habrá un filtro de las capacidades de cada uno y para nosotros la especialización es un factor determinante frente a las empresas generalistas.

¿En qué momento, de consolidación o expansión, se encuentran vuestras actividades en los mercados internacionales? ¿Puedes comentarnos proyectos y casos concretos?

Existen dos aspectos. Dentro del Plan de Internacionalización de la compañía que empezó hace dos años, se creó una sociedad en México, pensando ya en el mercado latino, y después se han llevado a cabo una serie de estrategias para poder orientarnos al mercado EMEA. 2009 va a suponer la consolidación de México donde hay unas expectativas de crecimiento que empiezan a consolidarse a pesar de la crisis. Este año será bueno para la compañía en México con dos o tres proyectos emblemáticos en grandes compañías mexicanas.

La tecnología española empieza a ser valorada y hoy en día tenemos proyectos emblemáticos en los países árabes y en Reino Unido para lo cual tenemos una oficina en Londres y una oficina virtual en Dubai. También tenemos un proyecto puntual en EEUU con TELVENT para aplicar el valor de

la seguridad a los sistemas que gestionan infraestructuras críticas.

Además de en México, la compañía se encuentra en Argentina con un partner, y tenemos dos o tres proyectos en Colombia y Chile en los que colaboramos directamente con partners.

A nivel de proyectos este año va a ser de consolidación y se está trabajando para la distribución de la tecnología de **S21sec** a través de canales internacionales. Este es un trabajo que espero nos permita definir correctamente la estrategia durante este año con el objetivo de que a partir del año 2010 se establezca un canal adecuado para trabajar con nuestra tecnología a través de partners en otros países.

Algunos expertos en seguridad opinan que Internet es un ámbito inseguro por definición, ya que en su origen no se pensó en la seguridad, y además, la guerra contra los cibercriminales y los casos asociados de fraude no hacen más que crecer día a día. ¿Estás de acuerdo con esta teoría, o por el contrario puedes darnos razones objetivas que la rebatan?

Lo que ocurre con Internet es que estamos hablando de un medio digital, de un medio democrático y anónimo, lo cual desde un punto de vista conceptual está bien. Desde el punto de vista de las oportunidades de negocio Internet es la gran oportunidad y desde los últimos años del siglo XX estamos viviendo esta revolución. Esta revolución está cambiando los modos de relación entre las personas y entre las organizaciones y ahí es donde aparece el riesgo, cuando ese cambio se hace masivo. Internet es un medio que permite pasar a un modelo de sociedad digital.

Nunca hemos pensado en seguridad porque nunca hemos caído en lo inseguras que eran nuestras redes internas y ha sido al salir a Internet cuando estamos viendo la necesidad de una Red de confianza, teniendo en cuenta que la mayoría de las amenazas son internas. Desde el punto de vista del fraude es mayor el fraude de las tarjetas que el fraude por Internet pero eso puede cambiar. Desde el punto de vista económico Internet es mucho más seguro que la vida digamos civil, pero está claro que hay que construir una Internet de confianza, con una serie de normas que eviten no solo el fraude sino también problemas como la pederastia. Internet tiene el problema de que "el malo" puede operar en la alegalidad actuando desde países sin normativas o saltando de un país a otro.

Internet es la gran oportunidad para las personas, las organizaciones y los negocios pero tiene que enfrentarse a las regulaciones para crear una Red de confianza. Espero que dentro de 25 años se hable de confianza y no de seguridad en Internet. Este es el gran reto de las personas, las empresas y los gobiernos. Eso no quiere decir que desaparezcan los riesgos, siempre los habrá, pero hay que saber por dónde se circula, hay que saber circular por Internet con confianza sabiendo con quién nos relacionamos para lo cual, además de herramientas, tanto a nivel personal como a nivel empresarial se necesita formación. En materia de seguridad, tanto ciudadana como empresarial, todos tenemos que asumir un cierto riesgo y hay que hacer un buen uso de Internet.

Esta última pregunta puedes considerarla delicada, pero no podemos eludirla: ¿Puedes comentarnos algún gran incidente de seguridad en el que S21sec haya intervenido ayudando a su solución? O, si lo prefieres, ¿puedes comentarnos igualmente algún incidente en seguridad bancaria?

(Se ríe) Bueno, contaré uno de fuera. Un banco indio tenía un agujero de seguridad en sus servidores y a través de ese agujero cinco millones de usuarios fueron infectados en menos de dos días y se obtuvieron sus datos confidenciales de acceso para hacer transacciones, para copiar sus tarjetas, etc. Esta es una realidad. Y de eso nos tenemos que ocupar todos. Utilizar conceptos de buenas prácticas, actualizar los sistemas, parchear las aplicaciones, trabajar con empresas solventes que nos aporten conocimiento… Y no olvidemos que a las entidades bancarias también se las ha defraudado simplemente llamando a un *call center* suplantando a un cuerpo de seguridad y obteniendo así información crítica. La seguridad no es sólo un concepto tecnológico sino que es un concepto que tiene procedimientos.

No tenemos más espacio, pero, ¿consideras que nos hemos dejado en el tintero alguna pregunta que te gustaría responder?

Los dirigentes políticos y empresariales de este país nos tenemos que concienciar de que las tecnologías, Internet, suponen una gran oportunidad para crear un modelo diferencial que nos permita crecer en el mundo de los negocios desde la innovación, sin olvidar inculcar a todos los ciudadanos lo importante que es trabajar en un entorno de confianza haciendo de la seguridad un hábito. No hay que bajar la guardia, hay que formarse, hay que utilizar correctamente la tecnología con procedimientos que nos permitan mitigar los riesgos y tener en cuenta que la seguridad es un medio para conseguir que funcione la economía, que funcionen las relaciones ciudadano-empresas-gobierno para ser un modelo a imitar por otros países.