



+ MUJERES DIRECTIVAS

Entrevista a María Antonia García

Responsable de Seguridad de la Información

IBERIA Líneas Aéreas de España

ENTREVISTA REALIZADA POR
Ricardo Cañizares

FOTOS
María Notario

MARÍA ANTONIA GARCÍA REDONDO es Licenciada en Ciencias Económicas y Empresariales, Master en Gestión Empresarial y Técnico de Aviación Comercial. Una excelente profesional con más de 30 años de experiencia, que ha desarrollado su brillante carrera en el negocio del transporte aéreo.

Actualmente es responsable de Seguridad de la Información en IBERIA Líneas Aéreas de España, cargo que desempeña desde 1993. Anteriormente ocupó puestos de gestión en diferentes unidades de negocio de la aerolínea. Así mismo es colaboradora habitual en grupos de trabajo de seguridad de la información, tanto a nivel nacional como internacional, y ha participado activamente en foros de legislación (Protección de Datos, Firma Electrónica, Comercio Electrónico, Propiedad Intelectual) y técnicos (Seguridad en entornos distribuidos, Seguridad en WI-FI).

¿Cuál fue el motivo por el que IBERIA consideró que este era un buen momento para iniciar el proyecto?



Realmente, lo que hemos hecho ha sido esperar a la publicación y aprobación por parte de AENOR de la UNE-ISO/IEC 27001, aunque lo cierto es que llevamos trabajando cinco años con el objetivo de implementar un SGSI. Bajo mi punto de vista, un estándar de seguridad no es más que una guía que aplica el sentido común y la experiencia; una certificación en el estándar es una garantía de que las cosas se están haciendo bien, pero el hecho de no estar certificado no tiene por qué implicar una gestión incorrecta de la seguridad, ni mucho menos. Dicho de otro modo: la certificación es imagen o, lo que es lo mismo, no sólo hay que ser bueno sino que además hay que parecerlo.

¿Cómo debe abordarse un proceso de esta magnitud?

Sin lugar a dudas, con aliados dentro de la Organización. Seguridad puede tener muy clara la utilidad de este proceso, pero necesita del apoyo de la Alta Dirección, así como de diversas Unidades de Negocio.

En el caso de IBERIA, ¿de qué aliados estaríamos hablando?

Nosotros tenemos constituido un Comité de Seguridad del que forman parte todas las Direcciones de la Compañía. Una de mis labores consiste en coordinar a estos Responsables de Seguridad, tanto en



lo referente a posibles dudas que les puedan surgir relacionadas con el estándar como en las acciones a efectuar. En nuestro caso debo reconocer que los comienzos no han sido tan duros, seguramente por el hecho de tratarse de un proyecto patrocinado por la Alta Dirección, que entre sus prioridades se encuentra la de ofrecer garantías de seguridad tanto a nuestros clientes como a nuestros empleados.

Ahora que menciona a los clientes y empleados, ¿en qué medida les va a afectar esta certificación?

Ciertamente, uno de los primeros pasos a dar en un proyecto de estas características es fijar el alcance. Tiene que ser claro y estar muy bien acotado. En nuestro caso, se ha decidido comenzar por la certificación de nuestra web iberia.com y del Portal del Empleado. Como hablábamos al principio, esta garantía refuerza la imagen de seguridad que en todo momento queremos transmitir a los

clientes, que realizan sus reservas y compras a través de la web, emiten su tarjeta de embarque... y lo mismo sucede con nuestros empleados, que actualmente realizan un 99% de sus gestiones con Recursos Humanos a través del portal, y queremos ofrecer la garantía de que sus datos están securizados, no es posible su captura ni, por tanto, su modificación... y un largo etcétera de posibles amenazas en las que todos podemos pensar cuando hacemos cualquier tipo de transacción a través de Internet. Dicho de otro modo: se trata de garantizar un buen gobierno de la seguridad respecto a clientes y empleados.

Según entiendo, su opinión es que a día de hoy esta certificación ya tiene el peso suficiente como para ser una garantía de imagen a todos los niveles.

Sin lugar a dudas, aunque, ciertamente, mi opinión es que en este punto el papel de AENOR es crucial, ya que deberían promover una

política de marketing dirigida a los usuarios finales, en la que se les incitase a exigir esta certificación.

En cualquier caso, cabe pensar que es cuestión de tiempo, como en su día sucedió con la norma ISO de calidad; hoy a nadie le extraña encontrar el sello de AENOR en la publicidad de cualquier empresa, independientemente del sector al que pertenezca. Incluso podría decirse que es algo que los usuarios exigimos, porque nos da una garantía de calidad. Pues bien, mi opinión es que en el corto / medio plazo sucederá un fenómeno similar con la ISO 27001, y nosotros queremos ser pioneros para anticiparnos al resto del mercado, que cada día es más competitivo.

Y, volviendo a las expectativas, aparte de la imagen, ¿destacarían algún otro beneficio derivado de la certificación?

Más que de la certificación en sí, destacarían expectativas derivadas de la implantación de un SGSI. Por



mencionar algunas de las que hemos estimado:

- Desde el punto de vista financiero, y dado que un SGSI debe entenderse como un proceso proactivo, parece lógico pensar que vamos a tener una reducción de costes derivados de los incidentes de seguridad.

- Desde el punto de vista humano, teniendo en cuenta que un SGSI al final lo que establece es la cultura de seguridad de la empresa, esperamos una mejora de la sensibilización del personal respecto a sus responsabilidades en la organización, al menos en lo que a seguridad se refiere.

- Desde el punto de vista normativo, un SGSI constituye una evidencia de que la Organización observa toda la legislación que le afecta.

- En lo referente a relaciones con terceros, el hecho disponer de una orientación clara de seguridad y un marco normativo nos ha permitido tener criterio a la hora de determinar qué proveedor cuenta con una mejor gestión de la seguridad de la información o, mejor dicho, cuál se aproxima más al modelo de nuestra Organización.

- Por último, la garantía de contar con una gestión eficiente de los riesgos sumada a la posibilidad de ofrecer una medida de nuestro nivel de seguridad.

¿Cuál es la situación actual del proyecto?

Si partimos del hecho de que nuestro enfoque de trabajo se adapta al ciclo de Deming, lo más correcto sería decir que ya hemos realizado esfuerzos en todas las fases, aunque todavía no tenemos cerrado el ciclo al 100% de forma automatizada.

¿Cuándo se inició realmente la fase de establecimiento del SGSI?

Para ser exactos, la fase de PLAN comenzó a finales de 2003, tomando como referencia la antigua ISO/IEC 17799:2000 con sus 127 controles, y actualmente estamos adaptando nuestro modelo de cálculo de riesgos a la nueva ISO 17799:2005, que define 133 controles, y estamos revisando nuestra medida del nivel de seguridad de los activos basándonos en este nuevo estándar.

¿A qué se refiere con el término "medida del nivel de seguridad"?

Para realizar un cálculo del nivel de riesgo lo más realista posible, nosotros medimos la seguridad en cinco dimensiones: aparte de las características que exige preservar la ISO 17799 (CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD), nosotros analizamos la AUTENTICIDAD y la AUDITABILIDAD. Esta medición se lleva a cabo desde dos puntos de vista: ideal (nivel al que nos gustaría llegar) y el real (situación actual). La diferencia viene dada por las vulnerabilidades que afectan a los diferentes activos, las cuales propician la materialización de amenazas, que a su vez generan un impacto en mi sistema, y ello se traduce en una degradación de los niveles de seguridad. Si a ello le sumamos el hecho de que existen dependencias entre los diferentes activos, en mayor o menor porcentaje, así como aquellos factores que pueden condicionar un determinado impacto (pensemos en el factor de reposición de un determinado recurso por ejemplo), lo cierto es que se obtiene una fórmula de cálculo del nivel de riesgo muy compleja.

¿De qué volumen de activos estaríamos hablando?

Depende del nivel de granularidad con el que se quiera analizar. Si por

activos entendemos procesos de negocio, el número es relativamente limitado. Ahora bien, si pensamos en las áreas funcionales que dan servicio a dichos procesos, y en que éstas a su vez se apoyan en sistemas de información, que en nuestro caso estaríamos hablando de un orden de 600 con sus más de mil interrelaciones, queda claro que estamos hablando de un volumen complejo.

¿Qué conclusión puede extraerse del Análisis de Riesgos de IBERIA?

Una muy clara y es que los problemas de seguridad más críticos rara vez son de carácter técnico. El verdadero problema normalmente es la gestión, y es que hay una cuestión que no debemos perder de vista: la tecnología siempre debe estar alineada con los objetivos de la organización; nunca al revés.

Ha indicado anteriormente que el ciclo no se encuentra automatizado al 100%. ¿En qué herramientas se apoya el SGSI?

En nuestro caso todas las herramientas son desarrollos a medida que se han generado según nuestras especificaciones. Mi opinión es que para este tipo de procesos es muy difícil adaptar una herramienta de mercado (a no ser que sea muy abierta, y en ese supuesto seguramente la parametrización sea muy compleja...), ya que cada negocio es diferente y, aunque los controles a implantar sean más o menos los mismos (todo ello teniendo en cuenta que las declaraciones de aplicabilidad pueden variar...), la interpretación que cada empresa hace no tiene por qué ser igual.

Según su experiencia, ¿qué tipo de perfil sería el más idóneo para



abordar un proyecto de estas características?

Como ya he dicho anteriormente, lo ideal es contar con expertos en todas y cada una de las áreas de negocio de la compañía y, cómo no, especialistas de seguridad de la información, asesores jurídicos, expertos en gestión de recursos humanos y auditores internos. Es decir, el equipo debe ser multidisciplinar y tener en todo momento un enfoque eminentemente práctico o, lo que es lo mismo, hay que procurar adaptar el SGSI a la Organización; la idea no es buscar un modelo teórico ideal y adaptar la empresa a él porque con toda seguridad no va a funcionar. Aunque dicho de esta forma puede

parecer algo evidente, un error muy común en este tipo de proyectos es precisamente partir con una visión demasiado perfeccionista. Es sinónimo de condenarlo al fracaso.

Por último, ¿en algún momento IBERIA ha contemplado la posibilidad de alinear ISO 27001, ITIL y COBIT?

Indirectamente sí. De hecho, me parece una sinergia posible y muy recomendable, ya que estaríamos combinando la seguridad, la excelencia en servicios y un modelo de gobierno de TI adecuado, todo ello como resultado de un solo proyecto, lo cual nos beneficia desde el punto de vista de ROI. Tiene su lógica, ya que hay

algo que nunca debemos perder de vista: la supervivencia a nivel empresarial se basa en una serie de puntos clave:

- Disponer de procesos correctamente definidos.
- Disponer de una infraestructura de TI robusta.
- Disponer de una estrategia de seguridad de la información definida, clara y adaptada a los procesos de negocio y a la infraestructura existente.

Ante este escenario, debe adoptarse un método de trabajo que asegure, como mínimo, el cumplimiento de estos puntos. Parece lógico pensar que la mejor alternativa es hacer uso de mejores prácticas que, al final, todas convergen en los temas de seguridad, como era de esperar. ♦