Deloitte.

Entrevista a Juan Luis Repiso, Vicepresidente y Director de Seguridad Corporativa de Airbus Group en España

"Para garantizar la seguridad todos tenemos que colaborar y compartir información de forma coordinada"

Juan Luis Repiso, ingeniero aeronáutico por la Universidad Politécnica de Madrid y Coronel del Cuerpo de Ingenieros del Ejército del Aire, tras desempeñar diferentes destinos relacionados con la seguridad e inteligencia, se incorporó en 2005 al Grupo Airbus en España.

A finales de febrero leíamos la noticia de que habéis incrementado la producción de la exitosa familia A320 de aviones comerciales para hacer frente a las más de 11.500 unidades vendidas, de las que lleváis entregadas más de la mitad. ¿Cuál es la clave del éxito de estos modelos?

En el ámbito aeronáutico, uno de los factores que más influye en el éxito de un modelo es el coste de operación y la fiabilidad del avión. La familia A320 es muy fiable, sobradamente probada, y con unos costes de operación óptimos a lo largo de todo su ciclo de vida. Airbus ha sabido vigilar la respuesta del cliente y adaptarse a sus expectativas, adaptando sus planes a sus necesidades. Esta es la clave del éxito de Airbus.

De hecho, en lo que está trabajando el Grupo, es en la implantación de un modelo "Neo", que es básicamente la adaptación del modelo al siglo XXI, haciéndolo más eficiente, con mejores motores y mejor aerodinámica.

Precisamente vuestros avances en investigación e innovación en aviones más eficientes en consumo os hace muy atractivos a vuestros clientes civiles, las aerolíneas. El I+D+i no es algo que precisamente se haga de un día para otro, ¿cómo protegéis vuestra inversión en propiedad intelectual para evitar que sea comprometida antes de que un proyecto termine de ver la luz?

Existe especial protección para los entornos técnicos, lo que llamamos las "joyas de la corona", tanto a nivel de seguridad física como lógica. Ahora bien, es importante tener en cuenta que esta especial protección no puede

"En el ámbito aeronáutico, uno de los factores que más influye en el éxito de un modelo es el coste de operación y la fiabilidad del avión"

limitar el funcionamiento del negocio, por lo que ocasionalmente hay que considerar excepciones; pero eso sí, siempre controladas.

Se persigue la correcta aplicación del control de acceso del personal a la mínima cantidad de información imprescindible para su trabajo (*Need to Know*). De esta necesidad surgen sistemas dedicados y segregados con características muy especiales y equipos confinados para temas y personas muy concretos.

Esta cultura de seguridad está arraigada en la organización y las personas que trabajan en los diferentes proyectos observan de manera inherente a sus labores del día a día estas medidas básicas de seguridad y protección de la información.

Pocas organizaciones tienen en su estructura una figura de responsable de seguridad integral de la información, ¿por qué os planteasteis su creación? ¿qué cubre una figura como esta (Personas, expatriados, diseños, etc.)? ¿qué servicios y funciones prestáis al grupo?
En primer lugar, la existencia de la figura de un director de seguridad integral – o lo que en el Grupo se llama *holistic security*- es lo que dicta la lógica. La seguridad debe entenderse como un elemento global de protección de los activos de información. Tiene que haber una cabeza visible que dé la cara ante la organización y las autoridades. No es asumible que en una organización haya seguridades paralelas, inconexas y descoordinadas. Adicionalmente, e igualmente importante, es la manera de cumplir los requisitos normativos y legales aplicables. El Director de Seguridad se corresponde con la figura del Jefe del Servicio de Protección que aparecía en la Orden Ministerial Comunicada 17/2001, y que aún hoy día conserva su sentido, e igualmente es lo que la reciente Ley de Seguridad Privada 5/2014 requiere para una empresa como la nuestra.

El Director de Seguridad es el único interlocutor oficial con las Fuerzas y Cuerpos de Seguridad del Estado (Ministerio del Interior), el Centro Nacional de Inteligencia (Ministerio de Presidencia) y la Dirección General de Armamento y Material (Ministerio de Defensa).

Es igualmente el responsable último de todas las medidas de protección de personal y activos de la empresa, que incluyen edificios, instalaciones, maquinaria, información, sistemas informáticos, productos etc. No obstante, determinadas funciones –que no responsabilidades– están delegadas en grupos y personas específicos tanto pertenecientes al Departamento de Seguridad Corporativa (control de accesos, programas clasificados, relaciones gubernamentales, seguridad de la información, gestión de crisis y seguridad contra incendios), como a otras áreas (seguridad informática, seguridad de producto, etc.) Junto con la cabeza, es imprescindible que los especialistas de seguridad con conocimiento del negocio y los técnicos de seguridad existentes en el Grupo actúen bajo la coordinación del Departamento de Seguridad Corporativa y mantengan una relación de dependencia funcional y reporting hacia él. Mantenemos esta estructura de trabajo con éxito desde hace más de 7 años.

Al fin y al cabo, la gestión de la seguridad es como gestionar una batalla, tiene que haber un responsable para "ganar" o "perder" los conflictos y evitar que dichas responsabilidades se diluyan. No sería concebible la existencia y actuación descoordinada de "organizaciones paralelas de seguridad".

En ocasiones tendemos a pensar que los nuevos riesgos asociados a las nuevas tecnologías (ciber riesgos) nos quedan un poco lejos de los procesos de negocio que gestionamos en las empresas de fabricación. Pero, ¿cómo de relevantes son para vosotros los ciber riesgos dentro de los riesgos de la organización? ¿Cómo consideráis que puede afectar a la imagen de Airbus si os vierais afectados por un ciberataque?
Los ciber riesgos están muy presentes en nuestra empresa. De hecho, ya en el año pasado, la ciberseguridad era uno de los ocho objetivos dictados por el presidente de la empresa, Tom Enders. No deja de ser sorprendente que un objetivo así figure en la lista de prioridades de una empresa industrial aeronáutica.

Somos muy conscientes de los riesgos económicos por pérdida de contratos, espionaje industrial, sabotaje, imagen, sanciones, descalificación… por eso ponemos todo nuestro empeño en combatir las ciberamenazas. Sirva el dato que en los últimos comités de seguridad dedicamos el 90% del tiempo hablando sobre estos riesgos.

Desde el punto de vista de vuestro negocio, ¿cuáles son las amenazas, relacionadas con estos nuevos riesgos, que más os preocupan? ¿Qué medidas estáis introduciendo para hacer frente a las estas nuevas amenazas?
Las amenazas más preocupantes son los potenciales ataques dirigidos del tipo APT (Amenaza Persistente Avanzada, *Advanced Persistent Threat*), que podrían perseguir el espionaje industrial (información de I+D), comercial (ofertas o contratos), información de personal. Otras amenazas que nos preocupan son los ataques de denegación de servicio (DoS) que puedan afectar a nuestra interconexión con socios, subcontratistas o clientes o ataques que podrían dar lugar a intrusión o sabotaje en los sistemas de control industrial de fabricación o a los sistemas financieros.

Respecto a las medidas existe un plan de mejora constante de la ciberseguridad global que persigue la instalación y mantenimiento de sistemas de protección actuales, la segmentación adecuada de las redes informáticas, centros de seguimiento y monitorización de la seguridad, equipos de alerta temprana, de respuesta de incidentes, gestión de crisis y, algo muy importante, la interconexión e intercambio de información permanente tanto dentro del grupo como de las Agencias de Seguridad Nacionales de los países copartícipes.

Alrededor de Airbus hay un ecosistema de proveedores y contratistas de todo tipo con los que tenéis que compartir información, ¿cómo gestionáis la cadena de proveedores, sobre todo desde el punto de vista de la seguridad?
Nuestros socios y proveedores son de indudable prestigio y están certificados adecuadamente para operar en el sector. Respecto a las subcontratas, existe distinta política en los sectores civil y militar. Mientras que en el civil, el personal subcontratado accede desde sus instalaciones y estas son objeto de auditorías por parte de Airbus, en el militar se recurre a la subcontratación in-situ, de modo que el personal opera en nuestras instalaciones y está sujeto a la normativa y control de seguridad de nuestra empresa.

¿Cómo de importante es el factor humano? ¿Cómo hacemos partícipes a todos los miembros de la organización de la importancia de la seguridad de la información?
Como ya he comentado, el factor humano es un elemento clave para nosotros. Estamos llevando a cabo frecuentemente campañas de concienciación. Además, en el sector militar, es muy frecuente la necesidad de habilitaciones oficiales para trabajar, lo cual implica una formación especial. A nivel de grupo, estamos realizando jornadas monográficas para todos los empleados, con charlas, talleres, etc., en lo que denominamos el *Airbus Security Day*.

Por ejemplo damos charlas sobre tácticas de ingeniería social a las secretarias de los directivos, para que estén preparadas ante diferentes técnicas que las pueden poner a prueba.

No obstante, la concienciación es como el derecho natural, es decir, "yo te explico las cosas para que tú comprendas cual es el modo de actuar razonable y beneficioso para ti y para la organización". Pero para que las normas se apliquen, debe existir también un derecho positivo, es decir, debe existir un régimen sancionador que se ponga en práctica en caso de incumplimiento.

Hace unos meses conocíamos la noticia de un cibersabotaje de una planta siderúrgica en Alemania que ha supuesto una parada de su cadena de producción. ¿Os planteáis el sabotaje de la cadena de producción mediante un ciberataque?

"La gestión de la seguridad es como gestionar una batalla, tiene que haber un responsable para 'ganar' o 'perder' los conflictos y evitar que dichas responsabilidades se diluyan"

Por supuesto que nos planteamos la posibilidad de sabotaje; y de muchos tipos, pero no vamos a dar ideas… Si Seguridad no valora un riesgo comete un error inadmisible.

Los riesgos son innumerables y hay que recoger todos los posibles. Y el procedimiento para gestionarlos es en esencia el estándar: un modelo de análisis que siempre parte de una identificación de bienes y daños una valoración del potencial impacto y de la probabilidad de que ocurra, y consecuentemente, una decisión de actuar para la atenuación del riesgo, para transferirlo si es posible o para asumirlo. Lógicamente son los parámetros económicos –retorno de la inversión en seguridad- los que priman en ella.

En tu experiencia ¿cómo hay que plantear la gestión de una crisis causada por una amenaza digital?
Un correcto procedimiento de gestión de crisis vale para todo, y eso lo tenemos bien definido. Nosotros tenemos un proceso de gestión de crisis, adaptado al Esquema Nacional de Seguridad, y perfectamente instrumentado.

Se estructura en tres principios fundamentales: conocer qué ha pasado, implantar una estructura que te permita en un momento determinado tomar decisiones –con gente que sepa lo que ha pasado y gente que pueda decidir-, y finalmente, informar, tanto hacia arriba como a los colaterales. El núcleo de la gestión de crisis en España lo integramos los responsables de Recursos Humanos, Comunicación, y yo mismo, que analizamos cada situación, y decidimos el equipo de gestión de crisis adecuado y si se realiza una gestión local o bien se escala.

Evidentemente, cada crisis involucra a diferentes equipos expertos, pero la coordinación siempre parte del mismo entorno. Ya hemos hablado de la necesidad de la Seguridad Integral. En particular, para las amenazas digitales existe un grupo trasnacional de respuesta a incidentes que dispone de la adecuada capacitación y experiencia. Pero como en cualquier entorno de guerra – y la ciberguerra lo es-, el enemigo desarrolla unas capacidades y nosotros tenemos que ser capaces de conocer y aplicar las correspondientes contramedidas.

En Airbus realizamos simulacros de seguridad para probar y entrenar nuestras capacidades de respuesta.

En el ámbito informático la gestión de la crisis es más técnica, pero en el momento en el que tienen impacto aspectos no técnicos, se produce automáticamente la activación de otros puntos del plan de gestión de crisis, como por ejemplo los relacionados con la imagen de la compañía.

Además de vuestra estructura para dar respuesta a los riesgos de seguridad a los que estáis expuestos, ¿cómo de relevante crees que es la colaboración con otras empresas de fabricación, organismos oficiales, etc. para estar preparados ante las amenazas?
La colaboración es esencial, y sólo será eficaz si está coordinada. Nosotros consideramos que otras empresas, sean de nuestro sector o no, dentro de unos márgenes de confianza, y aun siendo competidores, no son el enemigo. Por supuesto, mucho menos lo es la Administración. Todos tienen que colaborar y compartir información.

Por tanto, es nuestra voluntad, compartir y recibir información y ayuda porque el beneficio es para todos; y así lo hacemos. Pero como comentaba, tiene que ser bajo coordinación. Es ahí donde consideramos que ese papel lo debe realizar un organismo oficial, que actúe tutelando de manera neutral y que incluso pueda conservar el anonimato de las fuentes de información por cuestiones de sensibilidad, pero que a la vez sea capaz de transferir los indicadores de los incidentes o la experiencia al resto de la comunidad. La administración pública debe ser, por tanto, el punto focal.