Santa Cruz de Tenerife, 1 de septiembre de 2017

HackHotel 2017 expondrá estrategias y claves legales ante posibles brechas de seguridad de la información en el sector hotelero

El coloquio '¿Cuánto cuesta ser legal?' contará con expertos de RIU Hoteles, la Unidad de Criminalidad Informática del TS, la Universitat de València y la Asociación de Peritos Judiciales Informáticos

El nuevo Reglamento de Protección de Datos de la UE obligará a las empresas a comunicar en 72 horas sus brechas de seguridad y qué medidas correctivas aplicarán en tales casos para paliar los daños

HackHotel 2017 (www.hackhotel.es), I Congreso Nacional de Ciberseguridad Hotelera, que organiza la Asociación Hotelera y Extrahotelera de Tenerife, La Palma, La Gomera y El Hierro, **Ashotel**, expondrá las claves y aportará estrategias para evitar y para actuar ante posibles brechas en la seguridad de la información de las empresas hoteleras en general y, en particular, cuando estas brechas afecten a datos particulares. También se abordarán los posibles delitos informáticos en que se pueda incurrir como consecuencia de ciberataques y cómo reaccionar ante ellos de forma correcta y coherente con la normativa vigente. Será en la mesa coloquio '¿Cuánto cuesta ser legal?', moderada por la abogada **Noemí Brito.**

Brito, directora de Derecho Digital de Legistel e IT GRC (Information Technology Gobernance, Risk and Compliance) en Comtrust, contará en este debate con **Elvira Tejada de la Fuente**, fiscal de sala del Tribunal Supremo, delegada nacional de la Unidad de Criminalidad Informática; **Ángel Bahamontes**, presidente de la Asociación Nacional de Tasadores y Peritos Judiciales Informáticos (Antpji); **Ricard Martínez**, director de la Cátedra de Privacidad y Transformación Digital Microsoft Universitat de València; y **Águeda Borges**, responsable de los Servicios Jurídicos de RIU Canarias.

"Que el propio sector hotelero se pregunte qué puede hacer por mejorar la seguridad de la información bajo su responsabilidad y su ciberresiliencia a través de la organización de un congreso como **HackHotel** pone de manifiesto la importancia de estos temas e implica una decidida apuesta del sector por la mejora continua de su competitividad general", asegura la experta en Derecho Digital.

"La Unión Europea pivota su actual estrategia económica sobre la denominada economía de los datos", explica Brito, quien destaca el gran valor que para nuestra sociedad en general, y para el sector empresarial en particular, tiene la protección, análisis y explotación de todo ese conjunto de datos que se utilizan a diario. Su tratamiento está regulado por una serie de normativas europeas que deben conocerse para extraer todo el posible potencial asociado a esta información en beneficio empresarial con las máximas garantías posibles para los usuarios y clientes.

Como apunta Brito, “la ley puede operar como aliado competitivo si se conoce y aplica de forma inteligente, pudiendo inspirar y favorecer, incluso, nuevos modelos de negocio turísticos, por ejemplo, asociados al sector infomediario, muy ligado a la reutilización de la información propia o de terceros”.

Por otra parte, pronto deberá transponerse una nueva Directiva europea de Secretos Empresariales que refuerza la protección de la información en manos de las empresas (innovación, proyectos, fondo de comercio, etc.) que puede quedar en manos de ciberatacantes o terceros, incluyendo la propia competencia, si no se adoptan las adecuadas políticas y protocolos de seguridad.

Comunicar las brechas de seguridad

Y para el manejo de toda esa información es fundamental garantizar su seguridad, protección y, en caso de tratarse de datos personales, la privacidad. En este sentido, el próximo mes de mayo será de directa aplicación el Reglamento General de Protección de Datos impuesto por la UE y al que tendrán que adaptarse todas las empresas. Su incumplimiento puede acarrear la imposición de sanciones de hasta 20 millones de euros o el 4% del volumen de negocio total anual global de la empresa, la opción que comporte mayor cuantía.

Entre los aspectos que regulará esta norma, explica la abogada de Legistel, se establece “un plazo máximo de 72 horas para que cualquier entidad empresarial notifique a la autoridad de control (Agencia Española de Protección de Datos), y según qué casos a los usuarios, las brechas de seguridad de la información detectadas y qué medidas correctivas se van a aplicar”. Por lo que, además de las posibles multas asociadas a las infracciones que se cometan, “la empresa también podría exponerse a una importante crisis reputacional frente a los clientes que puede suponer, incluso, un mayor perjuicio que la propia multa”, añade.

Se trata de un reglamento muy estricto “pero con un lado positivo, que no es otro que permitir y animar a las empresas a aplicar fórmulas de autorregulación y códigos de conducta que les permita demostrar que van por el buen camino e, incluso, minimizar la posible responsabilidad jurídica asociada en casos de incumplimientos”, apunta Brito. El cumplimiento de la normativa puede ser también una oportunidad para que las empresas se diferencien en competitividad y generación de nuevos productos o servicios vinculados al tratamiento del Big Data hotelero y turístico asociado.

En este sentido, HackHotel “debe convertirse en lanzadera que permita a los establecimientos hoteleros trazar renovadas estrategias para la mejor y más segura explotación de los datos que manejan y obtener beneficio económico de ellos. Conocer los límites de la norma y ser coherentes con las necesidades y derechos de los usuarios permitirá avanzar de forma segura en el negocio”, considera Brito.

Empresas e instituciones patrocinadoras y colaboradoras

El apoyo empresarial e institucional para llevar a cabo HackHotel es vital, una implicación sin la que este congreso muy probablemente no sería posible. Ashotel ha contactado con unas 30 empresas para participar en las mesas redondas y

ponencias. Las confirmadas hoy son las siguientes: Telefónica, ElevenPaths, Aenor, S21sec, CSA, ATOS Canarias, CaixaBank, GF-TIC, AENA, CEAV, Availpro, Mirai, Extreme Network, NetHits Telecom, Noray Software, Globalan, Open Data Security, Meliá Hotels International, Mapfre España, RiskMedia Insurance Brokers o Legistel Comtrust.

Además, varias instituciones participarán en los contenidos del congreso. Son las siguientes: Instituto Nacional de Ciberseguridad (Incibe), Policía Nacional, Guardia Civil), Fiscalía, Confederación Española de Hoteles y Alojamientos Turísticos (CEHAT), Instituto Tecnológico Hotelero (ITH), Instituto Tecnológico y de Energías Renovables (ITER), Asociación Nacional de Tasadores y Peritos Judiciales Informáticos y la Universidad de Valencia. También apoyan como patrocinadores destacados el Gobierno de Canarias, el Cabildo de Tenerife, el Ayuntamiento de Santa Cruz de Tenerife y la Subdelegación del Gobierno en Santa Cruz de Tenerife.

Sobre HackHotel y ciberseguridad

HackHotel 2017 tendrá lugar los días 10 y 11 de octubre en el Auditorio de Tenerife Adán Martín de la capital tinerfeña y prevé la asistencia de varios centenares de profesionales. Nace por la **inquietud de los empresarios hoteleros** de las Islas Canarias, especialmente los que conforman Ashotel, ante los acontecimientos sucedidos en los últimos tiempos relacionados con la ciberseguridad en algunos establecimientos alojativos y otras empresas turísticas. El turismo es en Canarias el verdadero motor de su economía, representa un 32% de su PIB y más del 30% del empleo existente en las Islas está directa e indirectamente relacionado con el sector turístico.

La **ciberseguridad** es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Define todos los conceptos que rigen la seguridad a través de internet, como datos personales, información bancaria, claves, compras *online*… La cantidad de información que circula por internet es enorme y los riesgos se hacen patentes cada día con mayor facilidad para las personas de a pie, pero también para las empresas, las instituciones e incluso los países. El ciberentorno es cada día más grande y, precisamente, la ciberseguridad debe garantizar la seguridad de nuestros movimientos en la red.