EBOOK "CIBERSEGURIDAD EN EL SECTOR TURÍSTICO"

Andalucía lab

itrem

FIT CANARIAS FACTORÍA DE INNOVACIÓN TURÍSTICA

GENERALITAT VALENCIANA

INVAT·TUR

ITH INSTITUTO TECNOLÓGICO HOTELERO

eurecat Centre Tecnològic de Catalunya

tecnalia MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

turistec

vicomtech MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

SEGITTUR turismo e innovacion

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN

thinktur Plataforma Tecnológica del Turismo

ÍNDICE

PRESENTACIÓN

La Plataforma Tecnológica del Turismo, THINKTUR (www.thinktur.org), trata diariamente la innovación en materia turística, observando como las nuevas soluciones tecnológicas se aplican al sector, incrementando su productividad y competitividad, transformando su oferta y conectando a todos los usuarios del ámbito turístico.

Desde el año 2016, el grupo de trabajo de Centros Tecnológicos en Turismo decidió colaborar estrechamente aunando sinergias e iniciativas. Por ello, como primer paso, se elaboró de manera conjunta un ebook que identificara las principales tendencias tecnológicas en turismo. Tras los años, el ebook se ha convertido en una iniciativa conjunta que cada mes de enero publicamos y presentamos en el foro #techYdestino de FiturtechY, en el marco de la Feria internacional de Turismo FITUR.

En el año 2017, el ebook se enfocó en el análisis de una tecnología clave en el proceso de transformación de la industria, el Smart Data, aportando casos de éxito que mostraban la utilidad de esta tecnología en el sector. En la edición de 2018, el tema estuvo centrado en la Inteligencia Artificial, aportando iniciativas desarrolladas por los centros y sus asociados, y en 2019 el grupo de trabajo de Centros Tecnológicos en Turismo orientó la temática del ebook a la tecnología Blockchain, recogiendo las principales propuestas de utilización y casos de uso ya puestos en marcha por cada uno de los Centros o por alguno de sus asociados, sirviendo como marco de referencia para comenzar a incorporar dicha tecnología en la gestión empresarial.

Por otro lado, en 2020, el grupo se orientó en el Sistema de Inteligencia Turística (SIT), en el que cada centro aportó su experiencia en el desarrollo e implantación de estos sistemas, acompañados de casos de éxito que sirvieran de inspiración para la puesta en marcha de nuevos Sistemas de Inteligencia Turística en otros destinos. La última edición, en esta ocasión elaborada para el mes de mayo de 2021, no podía tratar sobre otro tema más relevante en el momento: Soluciones e iniciativas orientadas a la resiliencia turística, con objetivo de ayudar a empresas y destinos turísticos a paliar los efectos que la crisis del Covid-19 ha generado en la industria turística, un sector en el que la colaboración público-privada ha sido más importante que nunca.

Para esta nueva edición 2022 del ebook, se han querido destacar aquellas iniciativas y proyectos en materia de ciberseguridad, así como contextualizar la importancia de la seguridad digital en el sector turístico, una industria con gran cantidad de datos vulnerables y de gran interés para los ciberdelincuentes.

Por último, agradecer a las nueve entidades (Andalucía Lab, Fit Canarias, Invat·tur, Instituto de Turismo de la Región de Murcia - ITREM, Instituto Tecnológico Hotelero - ITH, Eurecat, Tecnalia, Turistec, Vicomtech y Segittur) su esfuerzo y dedicación en la creación de este ebook que refleja su aportación a la mejora de nuestro sector.

Álvaro Carrillo de Albornoz

Director general

Plataforma Tecnológica del Turismo THINKTUR e ITH.

INTRODUCCIÓN

Hasta el año 2019, España era la segunda potencia turística mundial, en la que, según datos del INE, recibió más de 80 millones de visitantes extranjeros en dicho año, y el sector representaba un 12 por ciento del PIB, además de dar empleo a más de 2 millones y medio de personas. Pero el impacto del COVID-19 ha sido especialmente duro en este ámbito.

Ahora toca adaptarse a la "nueva normalidad" y apostar un nuevo modelo. Y, por tanto, tal y como señalan muchos expertos, la pandemia ha provocado la aceleración de la adopción de este nuevo modelo, basado principalmente en la innovación y digitalización y sus cambios asociados, también en el sector turístico. Además, señalan como claves para su remontada, el impulso del trabajo remoto, la digitalización de todos los canales, la diferenciación de la oferta, la creación de un ecosistema de servicios con *partners* y socios para proporcionar una experiencia más amplia, la simplificación de los procesos para reducir costes y la apuesta por nuevas plataformas e infraestructuras.

Es necesario, por tanto, asegurar espacios y destinos para que se restablezca la confianza del viajero. Las soluciones digitales logran crear entornos seguros con playas, museos, restaurantes, hoteles y centros de ocio con protocolos de seguridad y elementos interconectados. La tecnología también permitirá hacer los viajes totalmente personalizables, a través del análisis inteligente de la información, adaptando las preferencias del viajero a una oferta turística determinada, gestionando eficazmente sus tiempos de espera de acceso, o simplificando los servicios.

Aún muchas empresas no tienen una estrategia clara sobre su desarrollo digital, pero es inevitable que deben concebir que un proceso de transformación de este tipo debe ser su palanca de crecimiento, y que, junto al establecimiento de una adecuada estrategia de ciberseguridad, serán la clave para romper esta gran barrera, para su adaptación al ecosistema digital y, en definitiva, contribuirán de forma crucial a su éxito en el sector turístico.

¿Qué es la ciberseguridad?

En primer lugar, vamos a conocer el término ciberseguridad, que se puede definir como la práctica de proteger y defender los ordenadores,

servidores, dispositivos móviles, los sistemas electrónicos, las redes de comunicaciones y los datos de ataques maliciosos o malintencionados (ISACA). El término se aplica en diferentes contextos y puede dividirse en algunas categorías comunes, como:

- La seguridad de red es la práctica de proteger una red informática de los atacantes, ya sean ataques dirigidos o por malware.
- La seguridad de las aplicaciones se enfoca en mantener el software y los dispositivos libres de amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger.
- La seguridad de la información protege la integridad y la privacidad de los datos.
- La seguridad operativa incluye los procesos y decisiones para manejar y proteger los recursos de datos. Se incluyen aquí los permisos que disponen los usuarios para acceder, así como el cómo y dónde pueden almacenarse o compartirse los datos.
- La recuperación ante desastres y la continuidad del negocio definen la forma en que una empresa responde a un incidente de ciberseguridad y volver a estar de forma totalmente operativa en el menor tiempo posible.
- La capacitación del usuario final aborda el factor de ciberseguridad más impredecible: las personas. Cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro.

La ciberseguridad es un proceso, por tanto, las técnicas para abordarla se deben testear y actualizar de forma periódica, ya que las propias amenazas cambian y evolucionan constantemente.

¿Cuál es el coste de la ciberseguridad para las empresas?

Según diferentes estudios publicados, las empresas realizaron pagos de *ransomware* en el año 2020 por valor de más de 400 millones de dólares en criptomonedas, aumentando más de un 300% si comparamos con su año predecesor. Sin embargo, el coste promedio para una empresa en términos de impacto financiero, tiempo de inactividad y coste de oportunidad es mucho mayor, soportando incluso pérdidas millonarias en ingresos posteriores al ciberataque, además del daño sufrido a la reputación de marca y al valor para los socios o accionistas.

En este marco, desde la Plataforma Tecnológica del Turismo - Thinktur, en colaboración con los Centros Tecnológicos del Turismo (Eurecat, Fit

Canarias Invat·tur, Itrem, Tecnalia, Turistec, Andalucia Lab, Vicomtech, ITH y Segittur), se ha querido promover una vez más la elaboración de un ebook, centrado en dar visibilidad a los riesgos a los que se expone el sector turístico en materia de ciberseguridad y los aspectos que todo negocio del sector debe tener en cuenta a la hora de diseñar un plan estratégico de seguridad digital, plan que, si no tienen, deberían comenzar a diseñarlo con ayuda de las recomendaciones y conocimientos que podrá adquirir gracias a las aportaciones de los centros tecnológicos participantes y de las empresas asociadas que han contribuido en este ebook.

Andalucía Lab es un departamento de la Empresa para la Gestión del Turismo y del Deporte de Andalucía que trabaja para construir un destino turístico más competitivo, impulsando las competencias digitales y tecnológicas de las miles de pequeñas empresas que componen el sector

Además, establece puentes entre el ámbito turístico y el tecnológico y que las instalaciones en Marbella sirvan de palanca para emprendedores y profesionales independientes

Av. Cibeles, 1
29604 Marbella (Málaga)
www.andalucialab.org

Turismo y Ciberespacio: el reto de la seguridad

El sector turístico en España ha crecido y se ha beneficiado por nuestra posición geoestratégica, geopolítica y geoeconómica en valores absolutos de competitividad. Esta situación nos ha favorecido durante años, además, se ha venido acompañando de mejoras en el posicionamiento de nuestros destinos y la comercialización, así como por los avances e inversiones centrados en la calidad y la mejora de las infraestructuras o la cualificación de los recursos humanos. Por otro lado, se ha avanzado en las oportunidades originadas por la aplicación y el uso de la tecnología, acercando los destinos a los clientes y apoyando y ayudando en la mejora de gestión en todo lo que ella conlleva.

Aunque hemos sufrido duramente el varapalo de la COVID, el sector sigue desarrollándose y debe buscar la diferenciación necesaria para incrementar la competitividad en un nuevo hábitat que ahora es hibrido. El mundo virtual y el físico se ha fundido y la digitalización y la hiperconectividad ahora deber ser una prioridad.

En este ámbito global y digital en el que las sociedades se están construyendo y crecen, vivimos un nuevo paradigma, un cambio explosivo e impactante que ya se venían vaticinando. Estamos siendo testigos de la desaparición de las fronteras entre los flujos virtuales de la red y la realidad física y así, la sociedad, la economía, el turismo en este ecosistema tan complejo.

Se ha creado un nuevo hábitat, **un nuevo destino** que está perfilando el mundo y el consumo. El ecosistema digital, la digitalización y el desarrollo del ciberespacio y sus características nos han llevado al aprovechamiento de múltiples oportunidades, pero también a enfréntanos a importantes retos y desafíos.

Por un lado, el sector se enfrenta a las exigencias de un mercado global que requiere de una fuerte tecnificación e innovación en pro de la competitividad y la disponibilidad de productos y servicios donde se premia la inmediatez y la información, y por otra, una disciplina que, sin ser nueva, está impactando directamente en los negocios de cualquier tipo y que es especialmente sensible para el turismo, **la seguridad**.

Sobre este último, ya no vale solo tener en cuenta los riesgos y amenazas convencionales a los que día a día se enfrenta el sector, sino que hace años que ha entrado en juego el **ciberespacio**. Un espacio anárquico donde no existen paredes, no existen fronteras; muta rápidamente y es altamente dinámico; prácticamente incontrolable; débilmente regulado y completamente global y accesible.

Así, con la aparición de internet de las cosas, el todo conectado, la realidad virtual, la geolocalización, la domótica aplicada a edificios inteligentes (inmotica), los miles y millones de servicios on line, los medios de pago inteligentes o la ingente cantidad de datos que se generan en el sector, las Smart cities, el Smart destination, la movilidad; la nube; los robots autónomos y la inteligencia artificial etc…, hemos ampliado nuestros niveles de exposición en el ciberespacio a amenazas que antes no habíamos considerado. A esto hay que añadir la vulnerabilidad de las infraestructuras que aseguran el mantenimiento de los servicios esenciales para la sociedad y que impactan de manera directa sobre el sector (la luz, el agua, el transporte, entre otros)

Sin darnos cuenta, hemos aumentado el número de puntos y las posibles formas en que los delincuentes, ahora ciberdelincuentes, pueden acceder a redes, a sistemas, a servicio cuyas acciones pueden tener consecuencias inesperadas. Los ciberataques están impactando sobre los intereses empresariales, el desarrollo del negocio o su continuidad, la reputación o la competitividad. Hemos de sumar a esto la falta de concienciación y sensibilización de las organizaciones y de sus empleados ante este problema.

El sector debe ser consciente de asegurar la gestión con sus clientes, integrar la tecnología de manera segura; mejorar la recopilación y seguridad de los datos que maneja e implementar la concienciación y la cultura de ciberseguridad haciéndose conocedor de los riesgos y amenazas que comporta la conectividad exponencial a la que se enfrenta, junto a la transformación digital en la está inmerso.

Ejemplos como el robo de información y datos de clientes por intrusiones en sus sistemas o las incorrectas configuraciones de las redes wifi abiertas , el fraude, el cifrado de la información de la empresa para pedir un rescate económico para recuperarla (ransonware), la posibilidad de intervenir en el sistema de control remoto de las habitaciones pudiendo manipular: termostatos; luces; televisores; persianas etc. o la simple

suplantación de una página web o su desfiguración no son casos de ciencia ficción. Sin olvidar la falta de concienciación de los usuarios de los sistemas o los ataques de ingeniería social.

En este sentido, es evidente la necesidad de que se tomen medidas para asegurar la protección contra una amplia gama de amenazas, como las descritas, pero teniendo en cuenta que el turismo tiene características que lo distinguen de otras industrias. La importancia de entender la seguridad como un elemento de crecimiento, competitividad y resiliencia del turismo, nos lleva a considerar la necesidad de **construir destinos altamente comprometidos y sinérgicos con la tecnología, pero también confiables un entorno que cambia rápidamente**.

Eurecat es una fundación privada sin ánimo de lucro que tiene por objetivo el impulso de la innovación en general y de I+D en particular en todos los sectores de actividad. En febrero de 2019, tras casi dos décadas en funcionamiento, la Fundación Parque Científico y Tecnológico de Turismo y Ocio de Cataluña se fusionó con Eurecat formando lo que se conoce hoy en día como el Departamento de Innovación Turística de Eurecat. Dicho Departamento está especializado en tres ámbitos principales.

El primero se refiere a los sistemas de información y a la creación de bases de datos para el conocimiento de la actividad turística en los destinos. En segundo lugar, desarrolla actividad relacionada con la inteligencia de mercados, la transferencia de conocimiento para agentes públicos y privados y el diseño de productos incluyendo el desarrollo de iniciativas innovadoras. Finalmente, el tercer ámbito de especialización se centra en el desarrollo tecnológico con la implementación de aplicaciones para la gestión de empresas turísticas y de destinos, así como para la mejora de la satisfacción del turista.

Joanot Martorell, 15, 43480 Vila-seca,Tarragona

www.eurecat.org

El Ransomware en el sector turístico

Las empresas del sector turístico dependen en gran medida de las tecnologías digitales para llevar a cabo las operaciones críticas de su negocio, incluido el procesamiento de pagos, la contabilidad o la gestión de reservas. En los hoteles, el uso de la tecnología se extiende incluso a la gestión del acceso a las habitaciones mediante tarjetas. Debido a esta dependencia que se está generando y se generará en los años venideros, las empresas del sector turístico deben de estar prevenidas y preparadas para que no sean víctimas de ciberataques y ciberincidentes, especialmente mediante el uso de ransomware.

El ransomware es un software malicioso (malware) que normalmente cifra los archivos almacenados en un sistema y borra los archivos originales, lo cual imposibilita su acceso a menos que se pague un rescate. Existen variantes que simplemente bloquean todo el sistema y luego le vende al usuario una contraseña para desbloquearlo. Otras variantes también roban los datos almacenados en el sistema antes de cifrarlos para así poder extorsionar a la víctima con la amenaza de hacer pública su información si no ha pagado el rescate.

En los últimos años hemos sido testigos de muchos ataques de este tipo, sin ir más lejos, el 4 de octubre de este año la cadena hotelera Meliá sufrió un ataque de ransomware que afectó a algunos de los hoteles de la cadena, uno de ellos el Meliá Barcelona Sky, cuya página web dejó estar disponible. Pero ya en 2016, los dueños de un hotel austriaco vieron cómo, hasta en cuatro ocasiones, perdían el control de las cerraduras electrónicas de las habitaciones y otros sistemas por culpa de diferentes ataques de ransomware.

Ransomware como servicio

Al igual que muchas otras tecnologías o herramientas, el ransomware es cada vez más fácil de encontrar y utilizar por los ciberdelincuentes de todo el mundo, los cuales ya no tienen que desarrollar su propio software de ransomware para lanzar un ataque e infectar sistemas de empresas a lo largo y ancho del planeta, sino que ahora hay grupos organizados que se dedican a desarrollar software de ransomware para posteriormente venderlo como un servicio (as a Service) a cualquier persona o grupo interesado. Muchos ya son los ejemplos de ataques de ransomware que han utilizado software desarrollado por terceros, por ejemplo, el

ransomware Ryuk, que infectó los sistemas del SEPE (Servicio Público de Empleo Estatal) y paralizó su actividad en todo el país durante semanas a principios de este año.

Al igual que los productos de software como servicio (SaaS, de sus siglas en inglés), el ransomware como servicio (RaaS, de sus siglas en inglés) proporciona un acceso relativamente barato (mucho menor de lo que cuesta desarrollarlo) y sencillo a este tipo de software malicioso a individuos, bandas u organizaciones que desean realizar un ataque de ransomware. Los proveedores de RaaS generalmente obtienen un beneficio del 20% al 30% de las ganancias generadas por el rescate que pagan las víctimas.

Pagar no debería ser una opción

En caso de ser víctima de un ataque de ransomware, no se recomienda en ningún caso pagar el rescate. Pagar no garantiza recuperar toda la información que te han cifrado, según el estudio de Sophos "El estado del ransomware 2021". Dicho estudio confirma que sólo el 8% de las empresas que pagan un rescate recuperan todos sus datos. Por otro lado, si realizas el pago es posible que seas objeto de futuros ataques de chantaje o extorsión. Al fin y al cabo, son delincuentes y ya saben que estás dispuesto a pagar. También se dan casos en los que los ciberdelincuentes solicitan una cifra mayor de rescate una vez has pagado la cifra que habían fijado inicialmente. Por último, y no menos importante, hemos de ser conscientes que pagar fomenta el negocio de los ciberdelincuentes.

¿Cómo podemos evitar ser la próxima víctima?

A día de hoy, la mayor parte de los ataques de ransomware consiguen infectar los sistemas de las víctimas a través de engaños de ingeniería social. Los ciberdelincuentes consiguen que los usuarios realicen una determinada acción para su interés mediante un engaño. Gracias a esta acción los ciberdelincuentes consiguen instalar el software malicioso en el sistema de la víctima y así infectarlo.

Para proteger las empresas, y en este caso, las turísticas, ante los ataques de ransomware, lo primero de todo es evitar ser víctima de engaños, y esto pasa por la concienciación y la formación de los trabajadores, colaboradores y proveedores de las empresas Todo este colectivo debe ser consciente de las serias consecuencias que puede

tener un ataque de este tipo y que conozcan las técnicas de ingeniería social más comunes para que no les cojan por sorpresa.

Por otro lado, es importante configurar y mantener los sistemas para evitar que sean vulnerables, y esto pasa por disponer también de software especialmente destinado a la protección de dispositivos, como los antivirus o antimalware, y mantenerlos siempre actualizados, al igual que el resto de los sistemas y software.

También es muy importante en este caso realizar copias de seguridad de los datos de forma periódica y almacenarlas en otro entorno, ya sea offline, en el cloud o en una red diferente, a la vez que se comprueba periódicamente que es posible restaurar las copias que se están realizando.

Minimizar la exposición de servicios internos a Internet, de manera que sea más difícil para los ciberdelincuentes infectarnos o que se propague la infección, también ayudará a prevenir este y otros muchos tipos de ciberataques. De la misma forma, contar con un corta fuegos actualizado y bien configurado puede evitar que los ciberdelincuentes, aunque ya se encuentren dentro de la red, puedan ejecutar sus acciones maliciosas y descargar el malware.

Por último, cabe destacar que otras acciones como controlar los accesos, utilizar segundos factores de autenticación, restringir el uso de aplicaciones o equipos no confiables o actuar rápido en caso de incidente, también ayudan a prevenir todo tipo de ataques.

GENERALITAT VALENCIANA

INVAT·TUR

Invat·tur es un centro dependiente de Turisme Comunitat Valenciana, cuya misión principal es la potenciación de la I+D+i en turismo como eje clave de la evolución de la Comunitat Valenciana hacia un modelo turístico inteligente.

Paseo Tolls nº 2, 03502 Benidorm (Alicante)

http://Invat·tur.gva.es/

https://www.youtube.com/user/Invat·tur

https://www.linkedin.com/company/invattur

https://twitter.com/GVAInvat·tur

https://www.facebook.com/Invat·tur/

Ciberseguridad en el turismo: una reflexión sobre los retos a los que se enfrenta el sector

Ante el escenario de reactivación y relanzamiento que afronta el sector turístico tras los peores momentos de la crisis derivada de la Covid-19, la digitalización de empresas y destinos turísticos aparece como una de las claves esenciales. La automatización de procesos y la aplicación de la Inteligencia Artificial, el Big Data y el procesamiento de datos masivos, la realidad virtual y extendida, las tecnologías contact-less, etc., surgen entre los aspectos clave de dicho proceso de digitalización, con un nexo común: la ciberseguridad.

Es evidente que la tecnología ha cambiado la forma de interactuar entre turistas y visitantes. Así, los clientes de un hotel pueden realizar el check-in a través de sus dispositivos móviles o mediante sistemas de reconocimiento facial; la sensorización de recursos turísticos se ha generalizado; los propios visitantes se han convertido en generadores de contenido, etc. En definitiva, ya no se concibe hoy día el turismo sin tecnología, con un crecimiento exponencial de flujos de información y dispositivos conectados que deriva en una cuestión no menos relevante: la seguridad de sistemas e infraestructuras y, lo que es más importante, la de turistas y visitantes. En este contexto, los desafíos para el sector son enormes y, probablemente, todavía no hemos sido capaces de visualizarlos.

¿Y cuáles son esos principales desafíos a los que se enfrentan empresas y destinos turísticos en materia de ciberseguridad?

Siendo el turístico uno de los sectores con mayor potencial de aplicación de tecnologías y procesos como la inteligencia artificial, la realidad aumentada y el procesamiento de datos masivos, esto lo convierte en un escenario perfecto para los ciberdelincuentes, que encuentran en estas tecnologías brechas digitales que aprovechar. El robo de información y los ataques a sistemas de información son algunos de los principales riesgos que corre el sector turístico, pues los datos se han convertido el nuevo oro del siglo XXI también para los ciberdelicuentes, que ven en la venta de datos en el mercado negro una vía rápida para la obtención de un alto rédito económico. De ahí que a medida que el sector avanza en su digitalización, también deba hacerlo en materia de seguridad pues prácticamente todo el customer journey y la cadena de valor del sector suponen la generación de datos relativa a clientes y empresas turísticas.

Los daños producidos por problemas derivados de ciberseguridad en las empresas y destinos turísticos van desde la pérdida de reputación o confianza por parte de los clientes, hasta la renovación de sistemas de información o la apertura de procesos legales, con la consecuente pérdida económica que ello supone.

Ninguna empresa ni destino turístico está exento de sufrir un problema con la ciberdelincuencia. Pero bien es cierto que el margen de error se puede reducir. Por eso, la ciberseguridad debe empezar a plantearse como un eje más en las estrategias de digitalización de las empresas, partiendo de medidas básicas como:

1. Implantación de un plan de seguridad que refleje peligros y posibles amenazas y conflictos, tanto en el ámbito informacional como en el operacional.
2. Definición de roles y responsabilidades en la empresa: restricción del acceso a los datos más sensibles y definición de la relación con terceros en materia de acceso a datos de clientes (limitar la cesión de datos y exigir la implantación de medidas de seguridad en el desarrollo de proyectos tecnológicos).
3. Formación y concienciación: el personal debe ser capaz de reconocer dichos riesgos que puedan dar lugar a incidentes, para así prevenirlos activamente y salvaguardar la seguridad de la información y de los sistemas asociados, y esto solo se consigue con una adecuada formación y concienciación.
4. Restricciones en las redes wifi: el acceso a Internet gratis es hoy en día un servicio básico, pero ello requiere de mayores niveles de seguridad, tanto en las redes internas (uso de trabajadores) como externas (uso de clientes).
5. Control sobre la evolución de la presencia online: la seguridad sobre los datos más sensibles de los clientes y de la empresa deben ir acompañados de medidas de vigilancia que permitan prever problemas y activar medidas para actuar ante ellos.

En definitiva, planificar en clave de ciberseguridad el proceso de digitalización y acompañarlo de la formación y concienciación adecuada son esenciales. Y es que, como decía Sun Tzu, la mejor victoria es vencer sin combatir, detectando vulnerabilidades en materia de ciberseguridad y previendo cualquier ataque, lo que permitirá mitigar y minimizar riesgos.

El Instituto Tecnológico Hotelero (ITH) es un centro de innovación para el sector hotelero y turístico, cuya misión es mejorar la competitividad del sector mediante la innovación y la tecnología; está adscrita a la Confederación Española de Hoteles y Alojamientos Turísticos (CEHAT).

Dentro de sus principales objetivos, se encuentra:

- Fomentar la cultura tecnológica y la innovación del sector con la finalidad de incrementar el valor de la oferta turística.
- Actuar como acelerador tecnológico.
- Difundir las mejores prácticas tecnológicas.
- Liderar proyectos de I+D+i relacionados con las infraestructuras hoteleras.
- Promover la cooperación empresarial en el área de la innovación tecnológica.

Las áreas de actuación sobre las cuales trabaja principalmente son la Innovación (nuevas tendencias, conceptos y servicios hoteleros novedosos), Tecnologías TIC, Procesos y Operaciones, y la Sostenibilidad y Eficiencia Energética, con dos ámbitos de trabajo; por un lado, la generación de conocimiento (difusión, sensibilización y formación) y la transferencia de soluciones innovadoras.

c/ Orense 32

28020 Madrid

www.ithotelero.com

La Ciberseguridad como elemento 360º en el negocio hotelero

Es una realidad que el 2021 se va a cerrar como el año con más ciberataques de la historia en España batiendo el récord que ya ostentaba 2020, y que el sector turístico se sitúa como el tercer sector más atacado en nuestro país. Por ello, el sector del alojamiento debe entender la ciberseguridad como un elemento 360º a aplicar en el entorno del negocio, con objetivo de reducir las innumerables vulnerabilidades y accesos en los que se localizan las diferentes brechas de seguridad, como son las infraestructuras TIC, redes, dispositivos (USBs, impresoras, etc.), domótica, etc., gracias a sistemas de protección adecuados, mantener la seguridad de los datos internos, de los proveedores y de los clientes así como asegurar transacciones de pago seguras, etc. Y para cuando el daño ya está hecho, el contar con una póliza de seguros en materia de ciberseguridad nos permitirá estar preparados para cumplir con la normativa vigente, poder continuar con la actividad y hacer frente a los daños causados.

Hay que tener en cuenta que cada vez tenemos más procesos en los que interviene la tecnología de manera activa en nuestros hoteles, y cada vez gestionamos más datos y de mayor valor. Para poder enfrentarnos con garantías de éxito a este desafío debemos conseguir que la protección de las redes en los hoteles sea transversal a todos los dispositivos y a todos los ámbitos del hotel. El modelo de custodia de datos ha cambiado, ahora además de custodiar los datos que el establecimiento necesita para su funcionamiento habitual, debemos de velar también por los datos que nuestros huéspedes llevan en sus dispositivos, para garantizar la seguridad y privacidad durante su estancia. Es necesario que valoremos más allá de las responsabilidades legales en las que podemos incurrir, también los posibles daños reputacionales que este tipo de incidentes pueden provocarnos. La protección de las redes debe ser integral, tanto perimetral (ataques desde exterior) como en profundidad (protección desde el interior) ya que un dispositivo comprometido puede afectar al resto. Para poder hacer de nuestro hotel un “ecosistema” seguro, necesitamos contar con partners en ciberseguridad con amplia experiencia en el sector hotelero, que nos ayuden a diseñar las redes desde su origen de una forma segura, y que puedan definir los posibles vectores de ataque en función de la tecnología y el contexto de cada hotel.

La política de seguridad de nuestro hotel debe de estar compuesta por una combinación de aplicaciones, procesos y fundamentalmente formación. Sabiendo que las personas son el eslabón más débil de esta cadena, la formación en seguridad como usuario de todas las personas de la organización es indispensable.

Es bastante habitual escuchar afirmaciones del tipo "¿Ciberseguridad? Para qué, si yo ya hago *backups* (copias de seguridad)" en los diferentes eventos y ferias del sector. Los ciberataques suelen generar importantes consecuencias económicas para intentar restablecer los sistemas, cierto es que un *backup* puede ayudar a paliarlas, pero no es el único problema que nos puede ocasionar, ¿y tu reputación? ¿y las sanciones económicas por incumplimiento del RGPD (Reglamento General de Protección de Datos)? Y aún más ¿y si en tu *backup* también está ya el virus?

En el sector turístico se maneja una gran cantidad de información sensible, unido a que solo un 5% de las compañías son consideradas expertas en ciberseguridad, lo convierte en un objetivo muy atractivo para ciberdelincuentes. Son muchos los riesgos a los que las empresas turísticas están expuestas (ransomware, phishing, etc.), sobre todo desde la rápida digitalización provocada por la pandemia, al permitir, gracias al teletrabajo, el acceso a los sistemas de información desde puntos y sistemas sin control o menos seguros que los propios implantados en las empresas. Por todo ello, la ciberseguridad debe ser considerada como un pilar básico dentro de cualquier plan estratégico de empresa cubriendo al menos dos aspectos fundamentales:

1. **Mitigar los riesgos de ciberseguridad** *(Identificar, Proteger, Detectar, Responder y Recuperar - NIST Cybersecurity Framework)*: implantando un plan director en ciberseguridad, realizando diagnósticos de seguridad que nos alerten de posibles amenazas, haciendo auditorías de cumplimiento, analizando aplicaciones e infraestructuras (incluyendo WIFIs), implantando soluciones tecnológicas de ciberseguridad, disponer de un BIA y un Plan de Continuidad de Negocio…
2. **Concienciación y Formación**: analizando las probabilidades de éxito realizando ataques simulados de phishing, módulos en entrenamiento interactivos, herramientas de *reporting* de incidentes e informes de resultados.

Backup, por supuesto que sí, pero además es necesario conocer, analizar y corregir las vulnerabilidades de tus sistemas, y formar y concienciar al

personal en aspectos de ciberseguridad, para poder garantizar un adecuado nivel de seguridad.

Por otro lado, las empresas deben establecer un proceso de pago seguro para las transacciones online con sus clientes, teniendo en cuenta aspectos tan importantes como:

- Establecer medidas de protección de ciberseguridad en los vectores de entrada que utilizan los ciberdelincuentes para ocasionar un incidente tecnológico, fraude o un secuestro (ransomware):
  - controles perimetrales seguridad y uso de protocolos de comunicación cifrados y autenticados.
  - controles en el correo electrónico y proxy de navegación que eviten la llegada de SPAM, correos fraudulentos, malware o enlaces maliciosos a los empleados.
  - sistemas actualizados y bastionados (configurados a nivel de seguridad).
  - aplicaciones de seguridad a nivel de sistema: basadas en firmas (EPP) y de detección y respuesta de amenazas (EDR).
- Establecer un proceso de recuperación eficaz después de un incidente de seguridad que permita recuperar la información y los sistemas de forma eficaz. Este proceso de recuperación y vuelta a la normalidad debe ser entrenado.

En relación con el proceso de pago seguro es importante destacar la Directiva de Servicios de Pago PSD2. PSD2 establece medidas de seguridad obligatorias para todos los comercios con el objetivo de reducir los niveles de fraude en las transacciones digitales, como por ejemplo la autenticación reforzada de clientes para compras online.

Finalmente, dada la gran dependencia tecnológica que tienen nuestras empresas actualmente, resulta de vital importancia contar con una póliza de ciberseguro que garantice la continuidad de nuestros negocios ante un incidente cibernético. Las consecuencias de un eventual incidente van mucho más allá de los daños en nuestros sistemas y bases de datos, y de los costes directos que supone recuperar la actividad normal del negocio. Estas consecuencias pueden implicar una pérdida de beneficios importante por la paralización de la actividad, reclamaciones cuantiosas por parte de usuarios, multas de la AEPD o daños reputacionales a la empresa. Por estos motivos, el ciberseguro constituye una capa clave de la seguridad digital, siendo el único eslabón de la cadena que contempla la

reparación económica por los daños directos y consecuenciales que puede tener un ataque o error en nuestros sistemas.

Hoy en día, se pueden encontrar paquetes con garantías muy completas en el mercado asegurador. Algunas de las más relevantes son:

- La respuesta a incidentes por parte de un equipo especializado.
- La responsabilidad civil frente a terceros por la gestión de sus datos o por publicaciones en internet.
- Las pérdidas económicas que puedan generarse por la interrupción de nuestros sistemas informáticos, e incluso las derivadas de incidentes que sufran los proveedores.
- Los incidentes de ciber extorsión, incluyendo el pago del rescate si es preciso.
- Los Fraudes informáticos y por robo de identidad o ingeniería social.

Incluso una empresa que cuente con las mejores herramientas de ciberseguridad y el mejor equipo de IT continúa teniendo una importante exposición a este tipo de riesgos. Concienciar a los empleados y contratar un ciberseguro son dos acciones sencillas y económicas que cualquier empresa puede implementar para minimizar el riesgo y operar en un ecosistema digital seguro.

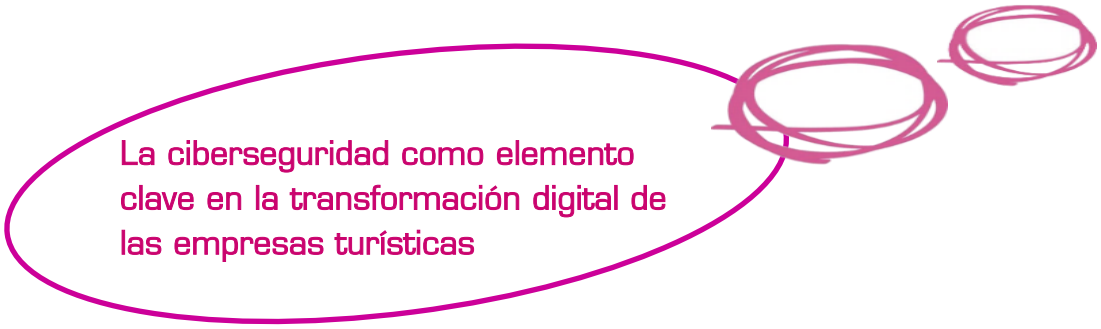
INSTITUTO DE TURISMO DE LA REGIÓN DE MURCIA

Entidad Pública Empresarial, creada por Ley (14/2012, de 27 de diciembre), que se ocupa de la ordenación, planificación, programación, dirección y coordinación de las competencias en materia de turismo de la Región de Murcia. Una de las competencias que desarrolla es la de Innovación, llevando a cabo acciones relacionadas con la gestión y desarrollo de programas para la implantación y gestión de programas tecnológicos en el sector turístico y en especial aquellos dirigidos a:

- Incrementar la competitividad de las empresas turísticas en los canales de venta online.
- El impulso a los destinos turísticos inteligentes en la Región de Murcia en
- La aplicación de las nuevas tecnologías al servicio del e-Turista.
- El desarrollo del sistema de Inteligencia turística regional.

Avd. Juana Jugán Nº 2, 30.006 Murcia.

www. Itrem.es



El sector turístico como una de las industrias objetivo top para los ciberdelincuentes.

El sector turístico se enfrenta a grandes amenazas en materia de ciberseguridad como son el robo de información para venderlo en el mercado negro, como los ataques que provocan la disrupción del negocio que no permiten a las empresas la prestación de sus servicios, y los ataques que afectan a la calidad del servicio ofertado y degradan la experiencia del usuario de este. Asimismo, el riesgo en el sector turístico se incrementa en su cadena de valor, en la que hay negocios de terceros que completan y complementan la propuesta ofertada a los usuarios, añadiendo nuevos riesgos y amenazas sobre la seguridad de los datos de sus clientes y, por tanto, de la propia empresa. Ya que en el desarrollo de la actividad de la compañía se gestiona una gran cantidad de información de los clientes, como datos personales y bancarios, un incidente de seguridad puede poner en riesgo la confidencialidad de esta información.

La pérdida de confianza de los clientes, daño a la reputación de la marca de nuestra compañía, pérdidas económicas y riesgos legales constituyen las principales consecuencias y los principales efectos de un ciberataque en la industria del sector turístico.

Ser consciente de las amenazas y conocerlas a fondo es esencial para poder evitarlas, y así proteger nuestros sistemas e información. Por ello se han publicado diversos manuales de uso como de buenas prácticas y guías de recomendaciones para el sector, como el publicado por el INCIBE este año, donde se detallan en profundidad algunas de ellas. Estos ciberataques los podemos englobar en las siguientes principales categorías:

- Amenazas al sitio web corporativo, donde las empresas del sector turístico y ocio ofrecen al potencial consumidor sus servicios y productos, y la indisponibilidad de dicho escaparate perjudica seriamente la continuidad del negocio. Las principales causas que provocan incidentes de seguridad en el sitio web corporativo son las

vulnerabilidades, las malas configuraciones, errores de diseño y fugas de información, el "defacement" o cambio de apariencia de la web, y los ataques de denegación del servicio (DoS).

- Amenazas en Redes Sociales, donde las compañías dan a conocer sus servicios de una manera más visual, moderna, interactiva y cercana a sus potenciales clientes, pueden sufrir campañas maliciosas de malware o phishing, incluso fraudes por suplantación de clientes y proveedores.
- Amenazas en redes de comunicaciones inalámbricas, que muchas compañías ofrecen para facilitar una conexión a internet gratuita en sus propias instalaciones a sus clientes. Algunos de sus riesgos, que extrañan tanto aspectos legales como técnicos, son la denegación del servicio (DoS); el denominado "Man-in-the-middle", donde un atacante se sitúa entre el origen y el destino de la información suplantando a una de las partes; los ataques de fuerza bruta, para intentar averiguar las claves de acceso; el MAC spoofing, donde el atacante suplanta la dirección MAC de un dispositivo; o el "eavesdropping", que consiste en la captura de tráfico de red no autorizado con el objetivo de hacerse con la información que se está transmitiendo por la red wifi.
- Amenazas a través del correo electrónico, que son las más comunes que afectan a las empresas del sector turístico. El fraude online, y su uso más habitual como es la suplantación de identidad por correo electrónico, es una de las ciberamenazas que más preocupa en la actualidad a las empresas. Los ciberdelincuentes utilizan la técnica denominada "e-mail spoofing" consistente en enviar correos con remitente falso para enviar spam, difundir malware o llevar a cabo ataques de phishing, suplantando incluso la identidad de directores o gerentes de la empresa, proveedores o clientes.
- Otras amenazas, como pueden ser los pagos con tarjetas robadas o ajenas, el fraude en las reservas vacacionales o las transferencias bancarias o cheques sin fondos.

Pese a que estos ataques crecen exponencialmente en la actualidad, muchos de estos riesgos pueden ser evitados, o al menos controlados, si aplicamos las siguientes medidas de seguridad:

- Seguridad en los datos: debemos reunir la información necesaria y limitar su acceso a terceros (partners, agencias de marketing, etc.)

realizando una gestión de registros, así como utilizar sistemas de respaldo y realizar copias de seguridad.

- Control de accesos a los datos más sensibles: restringimos el acceso de datos sensibles a los empleados y limitamos el número de accesos de administrador, así como la obligación de utilizar contraseñas de acceso robustas.
- Monitorización y segmentación de la Red: se aconseja monitorizar la Red 24x7 y localizar los datos más sensibles en un lugar más seguro, manteniendo actualizados los elementos de la red (firmware) y teniendo al día las actualizaciones de seguridad.
- Exigir medidas de seguridad a proveedores de servicios. Por ejemplo, debemos exigir seguridad de aplicaciones desarrolladas por terceros.
- Establecimiento de políticas estrictas en el apartado de cobros a clientes y pagos a proveedores, a través de plataformas electrónicas con reputación demostrada y seguridad actualizada.
- Establecimiento de medidas organizativas que complementen y den sentido a las medidas técnicas implantadas, como fomentar la formación y concienciación de los empleados.

Por tanto, las tecnologías como IoT, Big Data, 5G, edge computing, la nube y la ciberseguridad son los grandes protagonistas de la transformación digital del sector turístico y del ocio en España. Y, no cabe lugar a duda, que no existirá transformación digital sin el compañero ideal de la digitalización: la ciberseguridad.

SEGITTUR
turismo e innovacion

SEGITTUR, sociedad participada en su totalidad por la Administración General del Estado, tutelada por el Ministerio de Industria, Energía y Turismo del Gobierno de España, y a través de la Secretaría de Estado de Turismo, es la responsable de impulsar la innovación (I+D+i) en e l sector turístico español, tanto en el ámbito público (nuevos modelos y canales de promoción, gestión y creación de destinos inteligentes, etc.) como en el privado (apoyo a emprendedores, nuevos modelos de gestión sostenible y más competitivos, exportación de tecnología turística española, etc.).

Paseo de la Castellana nº135, Planta 16. 28046.
Madrid

www.segittur.es

El sector ante el reto de transformación digital segura

No cabe duda de que la transformación digital con la utilización de las tecnologías habilitadoras va a representar un importante aliciente para las empresas del sector del turismo y ocio por el aumento de productividad y rentabilidad que se espera lleven asociados. Algunas de estas tecnologías, también llamadas disruptivas, como el *cloud*, el *IoT* (*Internet of Things*), la inteligencia artificial, el análisis avanzado de datos (*big data*) o la robótica, se consideran la piedra angular de la digitalización con un efecto innovador en el desarrollo de productos, la aplicación en la mejora de los procesos o la gestación de originales modelos de negocio.

Con el uso cada vez más extendido de estas tecnologías y sus aplicaciones por empresas y usuarios se despliegan también nuevos escenarios para los ciberdelincuentes que aprovechan la potencia de la tecnología, y por otra parte sus vulnerabilidades, en su particular economía de escala. Así, vemos ingeniosos ataques a través de dispositivos conectados, la automatización de las campañas de phishing y el aumento de sus capacidades de evasión con IA (Inteligencia Artificial), o el alquiler en la nube de todo tipo de componentes para lanzar campañas de malware como servicio, por poner algunos ejemplos. Como siempre, los incidentes de seguridad llevan aparejados, aumentados ahora por estas tecnologías, pérdida de datos o de información sensible o de su confidencialidad, daños en la integridad de la información o de los sistemas, extorsión, fraude o fallos de disponibilidad; lo que supone casi siempre daños económicos y reputacionales, sin olvidar los posibles riesgos y perjuicios para los clientes.

Por ello, abordar estos cambios de espaldas a la ciberseguridad no es sensato, ni inteligente debido a los efectos devastadores que un incidente pudiera tener para la continuidad de las empresas del sector y para los usuarios que resulten afectados. En este sentido, es necesario abordar una transformación digital segura que aporte garantías, tanto a los usuarios como a los empleados y empresas del sector. Estas deberían contar con mecanismos de ciberresiliencia para soportar y superar con suficiente rapidez los posibles incidentes.

Por otra parte, el ecosistema del sector es un complejo entramado de empresas con tamaños y ámbitos de actividad distintos. Estas interrelaciones beneficiosas en el reparto de retornos económicos pueden serlo también para la defensa ante posibles incidentes de ciberseguridad o, por el contrario, convertirse en el canal de extensión de los posibles ataques. Es por esto por lo que se plantea que la estrategia de ciberseguridad del sector ha de contar con acciones coordinadas de todos los actores del mismo, y de estos con las FCSE (Fuerzas y Cuerpos de Seguridad del Estado) y los equipos de respuesta ante emergencias informáticas o CERT (*Computer Emergence Response Teams*) como INCIBE-CERT.

Además, es necesario empoderar al consumidor que pudiera estar aturdido por la volatilidad y complejidad de la tecnología, la cual va a tener o querer utilizar de forma ineludible, para darle el control necesario para proteger su privacidad y su seguridad en el uso, por ejemplo, de nuevos dispositivos que puedan ser útiles en aplicaciones del sector como wearables, domótica o vehículos autónomos. De esta forma, el sector se posiciona como un importante agente para la concienciación y sensibilización de los usuarios en un uso «inteligente» de la tecnología, con el apoyo de INCIBE, a través de los servicios de Protege tu Empresa y de la Oficina de Seguridad del Internauta (OSI).

El sector tiene ahora el doble desafío de abordar la transformación digital en paralelo a la incorporación de una gobernanza de la ciberseguridad que contemple no solo los tradicionales mecanismos internos de seguridad de las TIC, sino que se extienda a sus proveedores, colaboradores, *partners* y usuarios. Para ello, es necesario no sólo incorporar en nuestros planes estratégicos la ciberseguridad y la ciberresiliencia, e integrar la monitorización y la auditoría en el día a día de nuestros negocios, sino también extender nuestros requisitos de seguridad en los acuerdos de nivel de servicio y contratos tecnológicos en nuestro ecosistema, e irradiar concienciación en ciberseguridad a todos los que interactúen con nuestras empresas. Este es el objetivo de la reciente publicación conjunta de INCIBE y SEGITTUR: «*Ciberseguridad en el sector del turismo y ocio: Guía de recomendaciones para las empresas*», que animamos al lector a descargar, asimilar, aplicar y compartir para elevar la concienciación de empresarios, empleados y usuarios de los servicios del sector.

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

TECNALIA es el mayor centro de investigación aplicada y desarrollo tecnológico de España, un referente en Europa y miembro de Basque Research and Technology Alliance. Colaboramos con las empresas e instituciones para mejorar su competitividad, la calidad de vida de las personas y lograr un crecimiento sostenible. Lo hacemos gracias a personas apasionadas por la tecnología y comprometidas con la construcción de una sociedad mejor. Nuestra Misión es transformar investigación tecnológica en prosperidad. Nuestra Visión es ser agentes de transformación de las empresas y de la sociedad para su adaptación a los retos de un futuro en continua evolución.

Parque Científico y Tecnológico de Bizkaia
Edif. 700
48160 Derio (Bizkaia)
www.tecnalia.com

Brokel: Plataforma de compartición y explotación segura de datos sensibles

En los últimos años el interés por la economía del dato y la Inteligencia Artificial no ha dejado de crecer. Las empresas turísticas son conscientes del valor de los datos que generan, pero todavía no se está explotando suficientemente dicho valor por un cierto miedo o desconfianza a la hora de cederlos a terceros.

El acceso a un mayor conjunto de datos, más heterogéneo y diverso permitiría mejorar sustancialmente la explotación de datos y sería una forma de desarrollar la economía del dato, que se basa en compartir y poner en valor los datos de cada empresa con el fin de poder obtener un mayor beneficio común y premiar a aquellos que aporten más datos y de mayor valor al resto.

La compartición directa de datos entre dos empresas mediante acuerdos bilaterales está teniendo todavía un impacto muy limitado debido a esa desconfianza a la hora de compartir datos con terceros y por el miedo a perder el control sobre los mismos y que éstos sean compartidos y explotados indefinidamente.

Iniciativas como GAIA-X, apoyada en IDSA a nivel europeo, pretenden cambiar este ecosistema y aspiran a convertir a Europa en un referente en la compartición de datos. Precisamente la soberanía tecnológica y del dato propuesta bajo el paraguas de GAIA-X, abandera la ciberseguridad como la tecnología habilitadora clave para este nuevo ecosistema de datos. En este contexto, TECNALIA ha desarrollado la plataforma Brokel, que es una herramienta para dar respuesta a esta necesidad de las empresas, potenciar la economía del dato e impulsar la adopción de la Inteligencia Artificial.

Brokel es el resultado de una larga trayectoria en el desarrollo de tecnologías de privacidad dirigidas a la protección de los datos y los servicios digitales. El objetivo es garantizar la protección del dato a aquellas empresas que desean compartir o poner a disposición sus datos con terceros, sin perder la soberanía y control sobre su información. Al mismo tiempo, las tecnologías criptográficas aplicadas permitirán a los proveedores garantizar la confidencialidad de los algoritmos de Inteligencia Artificial con los que ofrecen servicios de optimización y predicción.

Las principales funcionalidades de Brokel son las siguientes:

- Realizar análisis estadísticos sobre los datos de clientes para obtener información de su interés (ej. perfil) sin llegar a conocer el detalle de dichos datos (ej. datos privados).
- Analizar datos del resto del sector y comparar su posicionamiento sin conocer el detalle de cada uno de los participantes o posibles competidores.
- Analizar las bases privadas de la administración pública y obtener conocimiento de su interés para actividades de marketing, segmentación, etc.
- Entrenar los algoritmos de Inteligencia Artificial sobre los datos del resto del sector o sus usuarios.
- Ofrecer servicios basados en dichos algoritmos o conocimiento experto sin desvelar su conocimiento y algoritmia.

Esta plataforma se beneficia de tecnologías como Criptografía Homomórfica, Secure Multi-party Computation o Blockchain para poder ofrecer una protección avanzada del dato y del algoritmo. Blockchain define la gobernanza de la infraestructura y se encarga de los incentivos, así como del permisionado y registro de acceso a datos por parte de aplicaciones/algoritmos o empresas. La capa de Secure Multi-party Computation permite a la plataforma la generación de nuevo conocimiento sobre datos de terceros, sin que dichos terceros deban en ningún momento mover sus datos de sus empresas, y sin que ninguna de las empresas conozca el dato o modelo unificado que han generado de forma conjunta. Por último, de cara a empresas que deseen ofrecer un servicio basado en los datos de terceros (mantenimiento predictivo, risk scoring, predicción de consumo energético, etc.) se utilizará criptografía homomórfica de cara a que dicho servicio se produzca siempre en un plano homomórfico (criptográfico) y que sean únicamente los beneficiarios de dichos datos quienes puedan descifrar el resultado de dicho servicio basado en el dato.

En la actualidad Brokel está siendo utilizado en diferentes proyectos piloto y su objetivo es posibilitar que las empresas puedan ser pioneras en la compartición y explotación segura y soberana de sus datos, y que ello juegue una ventaja competitiva en escenarios tan competitivos como el turismo.

turistec

Somos un clúster internacional dedicado a las Tecnologías de la Información y la Comunicación aplicadas al Turismo.

Fuimos el primer clúster industrial de Baleares y pioneros en España a la hora de concentrar el know how turístico.

Nuestro portfolio de clientes y partners concentra a los principales grupos turísticos, las PYMES del sector, emprendedores, la Universitat de les Illes Balears (UIB), centros de conocimiento y entidades para la excelencia y la calidad.

Nuestra apuesta conjunta es consolidar negocio, e innovar y evolucionar digitalmente la industria turística, aportando los beneficios socio económicos de nuestra actividad a los territorios donde operamos

Parc Bit, edificio Disset, A6, 07121 Palma, Illes Balears

www.turistec.org

Turistec technology tourism

Turistec.cluster

Racionalizar la planificación e inversión en la protección de la información

Racionalizar la planificación e inversión en la protección de la información, este es el consejo de BinauraMonlex, socio experto en ciberseguridad dentro del ecosistema empresarial de Touristec.

La ciberseguridad ya se ha convertido, por su propio peso, en una de las mayores preocupaciones de las empresas turísticas a lo largo de los últimos años. De hecho, el sector turístico ya es el **tercer sector más castigado a nivel mundial, por ciberataques e incidentes de seguridad**. La prensa internacional se hace eco de multitud de noticias relacionadas con ataques sufridos por las más importantes cadenas hoteleras pero, lo más importante, no conocemos los que han sufrido y sufrirán el resto de establecimientos hoteleros. Robos de tarjetas de crédito, ataques que paralizan las centrales de reservas, sustracción de datos personales de los huéspedes o secuestros informáticos (ransomware) son algunos de los principales ciberataques que se recogen en el sector hotelero en los últimos años.

Por todo ello, las organizaciones están invirtiendo en soluciones de ciberseguridad para defenderse de ataques, tales como antivirus, gestión de identidades, seguridad en tráfico de red o gestión de identidades, por poner unos pocos ejemplos de las tecnologías más solicitadas. En BinauraMonlex, empresa asociada a Turistec, creemos firmemente en adquirir tecnología suficiente para detectar y protegerse ante ciberataques, pero debemos establecer un matiz importante, previo a la inversión. **La clave está en la estrategia de ciberseguridad**, planificar la inversión en base a las necesidades y riesgos particulares de cada organización.

La estrategia en ciberseguridad queda perfectamente establecida con la implantación de un sistema de gestión de seguridad de la información, como la norma ISO 27001. La tendencia desde hace varios años en el sector turístico, y que se está incrementando a una velocidad enorme, es la elección de este estándar internacional entre otros sistemas de gestión como COBIT (Objetivos de Control para las Tecnologías de la Información y Relacionadas), NIST (Instituto Nacional de Estándares y Tecnología) o CIS

(Center for Internet Security). Algunos de los motivos de esta elección son:

- Pertenece a la International Organization for Standardization (ISO), por lo tanto, **no está mantenida por un grupo privado o gobierno.**
- **Es certificable**, a diferencia de normas capaces y reconocidas como la NIST de Estados Unidos. Por tanto, su implantación puede ir acompañada de un reconocimiento en forma de certificación oficial.
- Sirve como **base para desarrollar controles específicos** (Cloud, continuidad del negocio, ciberseguridad, etc.).
- **No está centrada únicamente en el departamento de TI**, sino en toda la organización o el alcance que se haya elegido para su implantación.

La utilización de la norma ISO 27001 permite establecer un gobierno de seguridad de la información, enlazando las estrategias de negocio con el funcionamiento del sistema de gestión de seguridad. De este modo, cualquier inversión en ciberseguridad que subyace del cumplimiento de las estrategias, políticas de organización o gestión de los riesgos, está plenamente analizada y planificada. Todo ello, con la imprescindible intervención de la dirección de la empresa que, como establece la propia norma, es consciente de la importancia de la ciberseguridad como elemento horizontal en todos los procesos de negocio.

Asimismo, la ISO 27001 nos servirá de base para otras normas de la misma familia, como la ISO 27799 que supone una extensión de controles para garantizar la privacidad de la información. La certificación en esta última norma supondrá a medio plazo, garantizar el cumplimiento del Reglamento General de Protección de Datos a clientes y partes interesadas. Este papel de garantía está siendo una **necesidad indiscutible dentro del sector turístico**; la altísima interconectividad entre los diferentes actores del sector, obliga a obtener el compromiso suficiente de que la información que transmitimos o almacenamos, se encuentra debidamente asegurada ante amenazas como los ciberataques. No olvidemos que, al tratarse de un estándar internacional, la mayor parte de las organizaciones conocen la norma ISO 27001 y solicitan su certificación como demostración de nuestra gestión de la seguridad, incluso antes de contratar con empresas, como medida de fiscalización y análisis de riesgos.

Así pues, desde BinauraMonlex y su especialización dentro del sector turístico, vemos la tendencia mundial en la implantación de la norma ISO 27001 como **método para racionalizar la planificación e inversión en ciberseguridad**, ganando en eficiencia y efectividad a la hora de implantar las correctas medidas de seguridad en la organización.

vicomtech

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

El centro tecnológico Vicomtech, adscrito a la Alianza Tecnológica BRTA, tiene por objeto contribuir activamente al beneficio de las empresas y la sociedad realizando investigación aplicada de excelencia en Inteligencia Artificial, Visual Computing y Tecnologías de Interacción, así como promocionar el talento de las personas. Tras veinte años de actividad, Vicomtech se ha situado como un agente tecnológico del tejido industrial vasco, español y mundial, impulsando la generación de conocimiento y la transferencia de tecnología, desarrollando prototipos de nuevos productos y facilitando nuevas líneas de negocio en cooperación con la industria, y soportados en Propiedad Intelectual original.

https://www.linkedin.com/company/vicomtech
https://twitter.com/Vicomtech
https://www.youtube.com/user/VICOMTech

Paseo Mikeletegi, 57,

20009 Donostia-San Sebastián

www.vicomtech.org

El turista, dueño de sus credenciales: la aplicación del concepto de Identidad Digital Auto-Soberana (SSI)

Tal y como ocurrió con los atentados del 11/S cuando se implementaron diferentes procesos y controles estrictos para recuperar la confianza del viajero y se estableció una "nueva normalidad" con un refuerzo en los controles aéreos, se espera que la pandemia lleve consigo un proceso similar para restablecer la confianza y la seguridad. En este contexto, diferentes organizaciones del ecosistema turístico están trabajando en la forma de integrar tecnologías DLT (Distributed Ledger Technology) para facilitar el intercambio de los datos relacionados con el estatus de inmunidad frente al Covid-19.

Uno de los elementos clave dentro de esta aproximación basada en la tecnología es el concepto de Self-Sovereign Identity (SSI), que incorpora los principios de propiedad y gestión de los datos de identidad con las tecnologías que implementan dichos principios. Aunque no existe una definición universal, el concepto principal se basa en otorgar a la persona el control y la autonomía sobre los datos de identidad, cómo se usan y quién los usa. Sólo dicha persona puede acceder y actualizar los datos, protegerlos (por ejemplo, mediante encriptación) y dar permisos a ciertos elementos de dicha información para un propósito concreto durante un tiempo limitado.

Las credenciales verificables (o Digital ID de SSI) son el equivalente digital a las credenciales que llevan las personas en sus carteras, como el permiso de conducción, el DNI o el pasaporte. Dichas credenciales digitales se almacenan en una App "cartera" en un dispositivo como el Smartphones, y se pueden compartir con otras "carteras" digitales que implementen estándares y protocolos compatibles.

Las reservas en las cadenas hoteleras son un buen ejemplo de aplicación de la utilización del concepto de SSI. Supongamos un cliente que realiza una reserva indicando sus preferencias, sus documentos identificativos y una tarjeta de crédito en un hotel una primera vez. Disponer de paquetes de credenciales digitales ya preparadas para realizar reservas hoteleras le permite volver a enviar dichos datos cada vez que realice una reserva en dicho hotel. De este modo, los hoteles no necesitan almacenar todos los datos de la identidad del cliente, sino únicamente aquellos necesarios por

temas de trazabilidad y recurrencia. Aunque sea necesario proteger estos datos para cumplir la GDPR y otros temas legales, este proceso sería más sencillo.

En este sentido, actualmente se están realizando pruebas piloto en unos 120 hoteles de tres marcas en Alemania financiados por la Administración Pública para utilizar las credenciales verificables de los empleados de cuatro grandes empresas en el proceso de check-in en estos hoteles. Los empleados acceden a la App "cartera", obtienen sus credenciales y las utilizan en el check-in mediante su dispositivo móvil.

Otro ejemplo actual es el IATA Travel Pass, que se basa en un Digital ID descentralizado de la empresa Evernym. Dicho Pass almacena datos encriptados como los resultados de las pruebas Covid o estado de la vacunación en el dispositivo móvil del viajero, de una forma descentralizada (sin que exista un repositorio central para esta información). Igualmente, se están probando esquemas innovadores de cifrado homomórfico, de modo que no sea necesario descifrarlos para su validación.

La SSI todavía necesita una validación extensa en el mercado y el apoyo para su implementación actual se limita a un grupo relativamente pequeño de empresas. Sin embargo, su potencial en el ecosistema turístico deberá ser seguido con interés, especialmente una vez que se publiquen los estándares y protocolos necesarios y se mejoren los retos asociados a la experiencia del usuario.

En la actualidad, el centro tecnológico Vicomtech está participando en varios proyectos de aplicación de esta tecnología. Así, dentro de la Red Cervera EGIDA, Vicomtech lidera el Paquete de Trabajo relacionado con la gestión de identidades para la protección de la información y la privacidad. Igualmente, está desarrollando proyectos piloto de gestión de identidades auto-soberanas para diferentes ecosistemas de aplicación en el proyecto TRUSTIND. Todos estos avances podrán aplicarse en un futuro al ecosistema turístico para su customización, validación y transferencia.

AUTORÍA DE LAS APORTACIONES

Introducción

ITREM

Juan Francisco Martínez Carrasco
Director
juanfra.martinez@carm.es

Entidad Colaboradora

TELEFÓNICA TECH
José Antonio Martínez Cano
Cybersecutiry Presales Engineer en
Telefónica Tech

Turismo y Ciberespacio: el reto de la Seguridad

ANDALUCÍA LAB

José Luis Córdoba
Director
jlcordoba@andalab.org
@Andalucialab

Entidad Colaboradora

ACCENTURE
Mar López Gil
Security Senior Manager
mar.lopez@accenture.com
@marobserva

El Ransomware en el sector turístico

EURECAT
Juan Caubet
Director of IT&OT Security Unit
juan.caubet@eurecat.org

Ciberseguridad en el turismo: una reflexión sobre los retos a los que se enfrenta el sector

INVATTUR
Francisco Juan Martínez
Director
juan_fra@gva.es

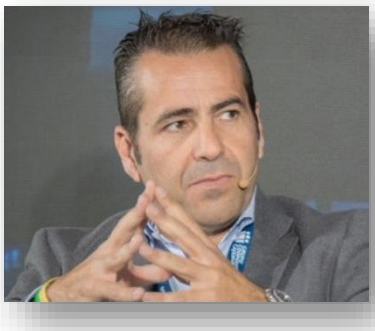
INVATTUR
David Giner Sánchez
Coordinador de Proyectos
giner_dav@gva.es

La Ciberseguridad como elemento 360º en el negocio hotelero

INSTITUTO TECNOLÓGICO HOTELERO
Paula Miralles
Área de Innovación
pmiralles@ithotelero.com
www.ithotelero.com

Entidades colaboradoras

CERIUM
Daniel Just
Hospitality Business Director
https://www.linkedin.com/in/djustmas/



GARCÍA ALAMÁN

Juan Carbajal
Director Comercial
juan@galaman.es

GMV
Joan Antoni Malonda
Tourism Business Development
jamalonda@gmv.com
www.gmv.com

CAJAMAR

Alejandro Ocete Martín

Ciberseguridad y Seguridad de la Información

Director Area

La ciberseguridad como elemento clave en la transformación digital de las empresas turísticas

ITREM

Juan Francisco Martínez Carrasco
Director
juanfra.martinez@carm.es

Entidad Colaboradora

TELEFÓNICA TECH

José Antonio Martínez Cano
Cybersecutiry Presales Engineer en
Telefónica Tech

Brokel: Plataforma de compartición y explotación segura de datos sensibles

TECNALIA

Jesús Herrero
Gestor Mercado Turismo
División ICT
jesus.herrero@tecnalia.com
@JesHerrero
@tecnalia

Oscar Lage
Responsable de Ciberseguridad y Blockchain
División ICT
oscar.lage@tecnalia.com
@Oscar_Lage
@tecnalia

Racionalizar la planificación e inversión en la protección de la información

TURISTEC

Jaume Monserrat
Presidente
turistec@turistec.org
@turistec

Entidad Colaboradora

BINAURA MONLEX

El sector ante el reto de transformación digital segura

SEGITTUR:
Victor Badorrey
Director de Relaciones Institucionales

INCIBE

Elisa Vivancos
Técnico de Ciberseguridad para empresas de INCIBE

El turista, dueño de sus credenciales: la aplicación del concepto de Identidad Digital Auto-Soberana (SSI)

VICOMTECH

María Teresa Linaza Saldaña
Directora de Promoción y Desarrollo institucional
mtlinaza@vicomtech.org

AGRADECIMIENTOS

Desde Thinktur y el resto de Centros tecnológicos que participan en esta iniciativa, queremos agradecer a nuestros socios y entidades colaboradoras que han participado en el desarrollo de los diferentes capítulos de este ebook, aportando su experto conocimiento sobre ciberseguridad en el sector turístico.

Asimismo, queremos dar un especial agradecimiento a INCIBE, el Instituto Nacional de Ciberseguridad de España por colaborar en esta iniciativa.

INCIBE trabaja para afianzar la confianza digital, elevar la ciberseguridad y la resiliencia y contribuir al mercado digital de manera que se impulse el uso seguro del ciberespacio en España.

El Instituto Nacional de Ciberseguridad de España (INCIBE), anteriormente Instituto Nacional de Tecnologías de la Comunicación, es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

Con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE contribuye a construir ciberseguridad a nivel nacional e internacional

La Plataforma Tecnológica del Turismo- Thinktur es un foro común en el cual los usuarios comparten información y conocimientos sobre la aplicación de la tecnología y la innovación para resolver los problemas reales y concretos del sector turístico.

Cuya finalidad es promover un Ecosistema de empresas Y destinos turísticos, junto a proveedores del sector turístico y entidades de investigación para fomentar la competitividad en el sector turístico mediante la difusión e implantación de la tecnología, innovación y sostenibilidad.

Teniendo presente que el objetivo último es contribuir al crecimiento sostenible del turismo, los objetivos específicos de la Plataforma ThinkTur son:

CREAR UNA RED: Crear una red de alianzas estratégicas e intelectuales con instituciones referentes de I+D+i españolas.

POTENCIAR LA FORMACIÓN: Impulsar acciones de formación y capacitación del sector.

INTERNACIONALIZACIÓN: Contribuir a la internacionalización del sector turístico español favoreciendo una presencia mayor en el entorno paneuropeo.

DEFINIR ESTRATEGIAS: Definición de la estrategia y elaboración de la Agenda Estratégica de Investigación.

I+D+I: Incentivar la participación de las empresas turísticas, sobre todo las pymes, en proyectos de I+D+i.

CREAR PROYECTOS: Generación de proyectos y traslado al mercado.

ASESORAMIENTO E INVESTIGACIÓN: Colaborar con las Administraciones Públicas y asesorarlas acerca de las principales líneas y prioridades tecnológicas de investigación que interesan al turismo.

Agradeciendo la colaboración de: