GUÍA
CIBER-RIESGOS DEL SECTOR HOTELERO

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO
AEI CLUSTER
Agrupaciones Empresariales Innovadoras
ITH
INSTITUTO TECNOLÓGICO HOTELERO
gmv
INNOVATING SOLUTIONS

ÍNDICE

1. Principales amenazas y riesgos del sector hotelero

La transformación digital en la industria hotelera ha brindado innumerables beneficios, mejorando la eficiencia operativa y elevando la experiencia del cliente. Sin embargo, este avance también ha expuesto al sector a una serie de amenazas cibernéticas que plantean desafíos significativos para la integridad de la información, la privacidad de los datos de los clientes, la reputación de los establecimientos y la resiliencia de los servicios hoteleros. Debido a amenazas crecientes como el ransomware o ataques cada vez más sofisticados de suplantación de identidad, la seguridad cibernética se ha convertido en un imperativo crítico para los hoteles en su transformación.

En este contexto, es esencial examinar detenidamente los vectores de ataque y las amenazas cibernéticas que acechan a la industria hotelera. Este análisis minucioso permite comprender los desafíos inminentes y desarrollar estrategias efectivas para mitigar estos riesgos. A medida que los hoteles buscan innovar y ofrecer experiencias personalizadas a sus huéspedes, la protección contra las amenazas digitales se convierte en un componente integral para garantizar no solo la seguridad, sino también la confianza y la satisfacción continua de sus clientes.

1.1 Tipos de ataque

En un mundo cada vez más interconectado, la industria hotelera se ha vuelto una víctima propensa a una variedad de ciberamenazas que comprometen la seguridad de los datos y la operatividad de los establecimientos. Estos ataques, ejecutados por ciberdelincuentes con diversas motivaciones, van desde técnicas de ingeniería social hasta ataques sofisticados a infraestructuras clave para el negocio.

1.1.1 Ransomware

El Ransomware es un tipo de software malicioso diseñado para bloquear el acceso a un sistema o archivos en un dispositivo hasta que se pague un rescate al atacante. En algunos casos el acceso se restablece una vez que se realiza el pago, pero no siempre se garantiza la recuperación total de los datos.

Modo de operación:

- Infección: El ransomware suele ingresar a un sistema a través de correos electrónicos de phishing, sitios web comprometidos o explotando vulnerabilidades en software desactualizado.
- Cifrado de datos: Una vez dentro del perímetro objetivo, el malware cifra archivos críticos o incluso todo el sistema, haciendo que sean inaccesibles para el usuario o la organización.
- Ransom y descifrado: El atacante exige el pago de un rescate a cambio de proporcionar la clave o herramienta necesaria para descifrar los archivos.

Impacto en la seguridad del hotel:

- Interrupción de operaciones: Un ataque de ransomware puede afectar los sistemas de gestión de reservas y registro check-in/check-out, interrumpiendo las operaciones normales del hotel.
- Pérdida de datos sensibles: Los hoteles almacenan datos e información personal de huéspedes, como nombres, direcciones, números de teléfono y datos de pago. Un ataque podría comprometer esta información, dificultando la operativa y causando incumplimientos regulatorios.
- Daño a la reputación: La pérdida de datos y la interrupción de servicios pueden afectar la confianza de los clientes, dañando la reputación del hotel.

La cadena de hoteles low cost Motel One víctima de un ataque de ransomware

Motel One Group, una cadena lowcost alemana que opera 90 hoteles en 13 países, incluido España, comunicó haber sido objetivo de un ciberataque en las últimas semanas. Aunque no se ha especificado la fecha concreta del ataque, la compañía emitió un comunicado de prensa el lunes 2 de octubre, aunque notificó el incidente vía Twitter el día 30 de septiembre.

La cadena, afirma que los atacantes obtuvieron acceso a los sistemas internos e intentaron ejecutar el ransomware, aunque, gracias a las medidas adoptadas, el impacto se redujo al mínimo, según un portavoz de la compañía. El portavoz también agregó que se accedió a los datos de un número desconocido de clientes, junto con los detalles de 150 tarjetas de crédito. Todos los titulares de dichas tarjetas afectadas fueron informados.

El grupo Stormous Ransomware ataca a una cadena hotelera española

Según la actividad de Darkweb detectada por el equipo de ThreatMon Threat Intelligence, el pasado mayo (2023) el grupo de *Ransomware* Stormous, agregó a su sitio de filtraciones al Hotel Mare en Dos Hermanas, España. El grupo desactivó los servicios del sitio web del hotel e, inmediatamente después, anunció vía Telegram que se tuvo que pagar un rescate para restablecer la normalidad de los servicios debido al aumento de la demanda del hotel a medida que se acercaba el verano.

Además del robo de la base de datos que contiene información sensible sobre reservas de habitaciones, usuarios, empleados y clientes, el grupo afirmó haber cifrado el contenido de las últimas 15 semanas en la base de datos de reservas.

Filtrados datos de clientes del grupo hotelero PortBlue

El 19 de junio de 2023, el grupo de *ransomware* 8BASE agregó a Port Blue Hotel Group, una cadena de hoteles situada en España, a su lista de víctimas, afirmando tener acceso a pasaportes y otros datos personales.

En total, se filtraron más de 300.000 pasaportes y otros datos personales. El atacante, 8BASE, fue responsable de más del 15% de todas las víctimas de *ransomware* el pasado mes de mayo.

Campaña de malware XWorm en reservas de hoteles

Durante el pasado mayo, un informe reveló que se había detectado una campaña de *phishing*, relacionada con reservas de hotel, para engañar a las víctimas. El objetivo era que dichas víctimas abriesen documentos maliciosos.

Para difundir los documentos señuelo, los atacantes utilizan tácticas de *phishing* que aprovechan la vulnerabilidad crítica de Windows, Follina (CVE-2022-30190) y ejecutan un script de PowerShell ofuscado, que deshabilita Microsoft Defender, establece la persistencia e inicia el binario que contiene XWorm.

- Consecuencias financieras: Además del rescate, los hoteles podrían enfrentar costos significativos para recuperar datos, fortalecer la seguridad y cumplir con requisitos legales.
- Cumplimiento normativo: Violaciones a regulaciones de protección de datos como el GDPR pueden resultar en sanciones financieras y daños a la imagen del hotel.

1.1.2 Mail del CEO

La suplantación de identidad, en particular el fraude del correo electrónico del CEO, se erige como una amenaza significativa para la industria hotelera. Este fenómeno implica una falsificación sofisticada donde los atacantes se hacen pasar por altos ejecutivos, como el CEO, con el propósito de engañar a los empleados.

Modo de operación:

El fraude del correo electrónico del CEO, también conocido como phishing ejecutivo, implica lo siguiente:

- Suplantación de identidad: Los atacantes se hacen pasar por el CEO u otros altos ejecutivos, aprovechando la confianza que los empleados depositan en las comunicaciones de sus superiores.
- Solicitud fraudulenta: Se envían correos electrónicos fraudulentos a empleados, solicitando acciones como transferencias de fondos, suministro de contraseñas, información bancaria o la revelación de documentos confidenciales.
- Engaño basado en confianza: La estrategia se basa en la relación jerárquica, donde los empleados, confiando en la autenticidad del remitente, pueden caer en la trampa y cumplir con las solicitudes maliciosas.

Impacto en la seguridad del hotel:

- Transferencia de fondos no autorizada: Los ataques pueden resultar en transferencias no autorizadas de fondos del hotel a cuentas controladas por los atacantes.
- Divulgación de información confidencial: Los empleados pueden verse inducidos a divulgar contraseñas y datos confidenciales, comprometiendo la seguridad de la red.
- Pérdida de datos financieros: Solicitudes de información bancaria pueden llevar a la pérdida de datos financieros sensibles.

1.1.3 Phishing e ingeniería social

Tanto el phishing como la ingeniería social representan tácticas insidiosas utilizadas por ciberdelincuentes para obtener información confidencial.

- **Phishing:** Técnica que involucra el uso de mensajes fraudulentos, como correos electrónicos o mensajes, que parecen legítimos para engañar a las personas y obtener información confidencial.
- **Ingeniería social:** Táctica que implica la manipulación psicológica de individuos para persuadirlos a revelar información confidencial, como contraseñas o datos personales.

Modo de operación:

- Correos electrónicos falsos: Los atacantes envían correos electrónicos que imitan a entidades legítimas, solicitando a los destinatarios que revelen información sensible.
- Mensajes engañosos: Utilización de mensajes persuasivos a través de diversos canales de comunicación, como mensajes de texto, redes sociales o aplicaciones de mensajería.
- Llamadas telefónicas fraudulentas: Los ciberdelincuentes pueden realizar llamadas haciéndose pasar por personal de confianza para obtener información.

Impacto en la seguridad del hotel:

- Fuga de datos de huéspedes: El Phishing dirigido a empleados del hotel puede resultar en la divulgación de correos de reserva de huéspedes.
- Acceso no autorizado a sistemas internos: La Ingeniería social puede llevar a que empleados divulguen contraseñas, permitiendo acceso no autorizado a sistemas internos.
- Fraude financiero: La obtención de datos bancarios a través de tácticas de phishing puede resultar en fraudes financieros.

1.1.4 DoS (Ataque de denegación de servicio)

Un ataque de Denegación de Servicio (DoS) es una forma de ataque cibernético diseñada para sobrecargar los recursos de un sistema, lo que resulta en la interrupción de servicios y la negación del acceso a usuarios legítimos. Este tipo de ataque tiene como objetivo principal afectar la disponibilidad y el rendimiento de los sistemas, dejándolos inoperables temporalmente.

Modo de operación:

- Generación masiva de solicitudes: Los atacantes inundan el sistema objetivo con una gran cantidad de solicitudes de servicio simultáneas. Estas solicitudes pueden ser de diversas formas, como solicitudes de conexión, solicitudes de recursos o tráfico de red adicional.
- Saturación de recursos: La avalancha de solicitudes masivas abruma los recursos del sistema, como ancho de banda, capacidad de procesamiento o memoria. Esto provoca una disminución significativa en la capacidad del sistema para manejar solicitudes legítimas.
- Impacto en la disponibilidad: Como resultado, los usuarios legítimos encuentran dificultades o son incapaces de acceder a los servicios normales del sistema, ya que este está ocupado procesando las solicitudes maliciosas.

Impacto en la seguridad del hotel:

- Interrupción de servicios online: Un ataque DoS podría afectar los servicios en línea de un hotel, como la plataforma de reservas y el sistema de gestión de clientes, impidiendo que los huéspedes realicen reservas o accedan a información crítica.
- Sobrecarga en sistemas de check-in/check-out: Los sistemas de registro y salida podrían verse afectados, causando demoras y problemas en la experiencia del cliente.
- Disminución de la calidad del servicio: La interrupción de servicios clave puede afectar negativamente la percepción del cliente sobre la calidad del servicio ofrecido por el hotel.

1.1.5 Ataques a sistemas críticos

Los ataques dirigidos a sistemas críticos, como los sistemas de reserva en línea, representan una seria amenaza para la integridad operativa y la seguridad de la información en la industria hotelera. Estos ataques tienen el potencial de comprometer datos confidenciales, manipular reservas e incluso interrumpir la funcionalidad normal de sistemas vitales para la operación hotelera.

Modo de operación:

- Manipulación de reservas: Un atacante podría acceder al sistema de reservas en línea y realizar cambios no autorizados, como la cancelación de reservas legítimas o la creación de reservas falsas. Esto no solo afectaría la operación diaria, sino que también podría resultar en pérdida de ingresos y daño a la reputación.
- Acceso a datos confidenciales: Los sistemas críticos contienen información sensible, como datos de clientes, información de pago y detalles de reservas. Un ataque exitoso podría comprometer esta información, lo que podría llevar a problemas de privacidad y violaciones regulatorias.
- Interrupción de funcionalidad: Desactivar o interrumpir la funcionalidad de los sistemas críticos, como el sistema de gestión de reservas, podría causar caos operativo. Esto afectaría la capacidad del hotel para realizar operaciones clave, como el check-in/check-out, y podría generar pérdida de confianza por parte de los clientes.

Impacto en la seguridad del hotel:

- Pérdida de ingresos: La manipulación de reservas podría resultar en la pérdida de ingresos directos, especialmente si se cancelan reservas válidas o se realizan reservas falsas que bloquean la disponibilidad real.
- Daño a la reputación: Los clientes afectados por cambios no autorizados en sus reservas pueden experimentar frustración y desconfianza, lo que afecta negativamente la reputación del hotel.
- Problemas de privacidad: La violación de datos personales y de pago puede tener consecuencias legales y afectar la confianza de los clientes en la capacidad del hotel para proteger su información.

Un hotel salamantino, entre las primeras víctimas de 3AM

El 22 de septiembre de 2023 el grupo de ransomware 3AM (ThreeAM) añadió al hotel salamantino Hacienda Zorita Wine Hotel & Spa a su sitio de filtraciones en la Dark Web. Por el momento, se ha publicado el 80% de la información extraída por los actores de amenaza, entre la que se encuentran facturas, fotos de eventos y correos corporativos.
3AM está escrito en Rust y es una familia de malware nueva. Los primeros análisis apuntan a que este ransomware solo se ha utilizado de forma limitada y de manera alternativa cuando los mecanismos de defensa bloquean LockBit, uno de los ransomware más activos en los últimos años.

Piden dos años de cárcel por suplantar la identidad de una directora de hotel y robar dinero

la Fiscalía de Granada ha solicitado una pena de dos años de prisión para dos hombres acusados de estafar más de 38.000€ obtenidos de forma fraudulenta mediante la suplantación de la directora comercial de 2 hoteles situados en la estación de esquí de Sierra Nevada.
El incidente se produjo el 1 de marzo de 2020, cuando los individuos atacaron la cuenta de correo electrónico de esta directora para suplantar su identidad y tras lograrlo, escribieron por correo a una tercera empleada pidiéndole que abonara un pago pendiente a la cuenta de los acusados.

Rusia ataca a empresas turísticas españolas por el apoyo a Ucrania

Más de una decena de empresas turísticas españolas sufrieron, durante la jornada del jueves 27 de julio de 2023, ciberataques de Rusia. Estos ataques fueron protagonizados por NoName057, organización que estuvo días atacando objetivos en nuestro país.

Con esta campaña, los hackers buscaban desestabilizar el principal motor de la economía española en plena temporada alta, dejando fuera de servicio las páginas web de varias instituciones y empresas turísticas. Entre las víctimas, se encuentran portales de información como Spain.info o las webs de turismo de Madrid y Barcelona. Varios sitios digitales de diversos hoteles también sufrieron caídas: Paradores, Riu, Majestic, Petit Palace, Only You, Catalonia Hotels & Resorts y, por último, las páginas de reservas de alojamiento Reservalis y Best Hotels. Algunos de los afectados sufrieron disrupciones temporales del servicio.

Gipuzkoa detecta los primeros ciberataques a clientes de hoteles a través de reservas

Los delitos se produjeron durante la primera semana de enero de 2023, detectando ciberataques a clientes de varios hoteles de la zona mediante phishing. Tras las pertinentes denuncias y adopción de medidas de seguridad, el sector indicó que no se habían producido más incidentes. Los ciberdelincuentes utilizaron la apariencia de agencias intermediarias como Booking para generar confusión sobre la reserva y el abono de las mismas, según confirmaron al Diario Vasco fuentes de la Asociación Hoteles de Gipuzkoa. Los atacantes se valían de esa falsa apariencia para redirigir las reservas a otros hoteles, con lo que se activaba el engaño y aprovechaban para hacerse con el dinero.

1.1.6 Ataques a la Wi-Fi del hotel

1. Man in the Middle (MitM)

Este tipo de ataque implica que un atacante se interpone en la comunicación entre dos partes, actuando como intermediario sin ser detectado. En el contexto de la red Wi-Fi del hotel, un atacante podría interceptar y modificar la comunicación entre los dispositivos de los huéspedes y la red, comprometiendo la confidencialidad de los datos.

Impacto en la seguridad del hotel:

- Violación de privacidad: Los datos sensibles, como información de inicio de sesión y datos personales transmitidos a través de la red, podrían ser accesibles para el atacante.
- Suplantación de identidad: El atacante podría realizar actividades maliciosas en nombre de los huéspedes, comprometiendo su identidad en línea.

2. Dark Hotel Hacking

Este enfoque implica ataques dirigidos a usuarios específicos mientras se alojan en un hotel. Los atacantes pueden comprometer la red del hotel para acceder a dispositivos de huéspedes específicos, aprovechando vulnerabilidades en sus sistemas.

Impacto en la seguridad del hotel:

- Acceso no autorizado: Los atacantes podrían obtener acceso no autorizado a dispositivos de huéspedes, lo que podría resultar en la pérdida de datos sensibles o la instalación de malware.
- Riesgo de fuga de información: La información empresarial o personal almacenada en dispositivos de huéspedes podría estar en riesgo.

3. Eavesdropping

En este tipo de ataque, un tercero no autorizado escucha las comunicaciones entre dispositivos en la red Wi-Fi. Los atacantes podrían capturar datos transmitidos, como contraseñas o información financiera.

Impacto en la seguridad del hotel:

- Compromiso de datos sensibles: La información transmitida, como detalles de tarjetas de crédito o información de reserva, podría ser comprometida, afectando la confianza del cliente.
- Violación de políticas de privacidad: El hotel podría enfrentar consecuencias legales y daño a su reputación si se violan las políticas de privacidad.

1.1.7 Insiders maliciosos

Los insiders maliciosos son empleados descontentos que representan una amenaza desde dentro de la organización. Dada la naturaleza de alta rotación en la industria hotelera, donde los empleados pueden tener acceso a información confidencial, la amenaza de insiders malintencionados se vuelve significativa. Estos actores internos pueden realizar actividades perjudiciales, como robo de datos, sabotaje o venta de información a terceros.

Impacto en la seguridad del hotel:

- Fuga de información confidencial: Los insiders maliciosos pueden acceder y filtrar información confidencial de los sistemas del hotel, comprometiendo la privacidad de los huéspedes y la reputación del establecimiento.
- Sabotaje de operaciones: La manipulación de sistemas internos puede conducir a interrupciones operativas, afectando reservas, servicios y la experiencia general del cliente.
- Venta de datos a terceros: Los empleados desleales podrían lucrarse vendiendo datos sensibles a competidores u otras entidades malintencionadas.

1.1.8 Ataques a la cadena de suministro

Los ataques a la cadena de suministro en el sector hotelero representan una amenaza que se centra en comprometer la integridad y seguridad de los sistemas utilizados en diversas áreas de la operación hotelera. Dada la descentralización en este sector, que abarca desde el punto de venta hasta la gestión de la propiedad, cada elemento de la cadena de suministro se convierte en un punto de entrada potencial para los atacantes.

Impacto en la seguridad del hotel:

- Compromiso de sistemas clave: Los atacantes pueden infiltrarse en sistemas clave utilizados en la gestión de reservas, control de acceso, sistemas de pago y otras áreas críticas de la operación hotelera.
- Interrupciones operativas: Los ataques a la cadena de suministro pueden resultar en interrupciones operativas, afectando la disponibilidad de servicios, reservas y la experiencia general del cliente.
- Fuga de información: Los atacantes podrían acceder a información confidencial, incluyendo datos de huéspedes, y utilizarla con fines maliciosos o venderla en el mercado negro.
- Daño a la reputación: Si se compromete la integridad de la cadena de suministro, puede producirse la pérdida de confianza de los clientes y dañar la reputación del hotel.

1.1.9 Ataques a páginas web

Los ataques a páginas web en el sector hotelero son acciones perpetradas por atacantes no autorizados que buscan comprometer la integridad de las páginas web de un hotel. Estos ataques pueden implicar cambios en la estructura de la página, la creación de sitios web falsos o el clonado exacto de la página legítima del hotel. El propósito principal es engañar a los visitantes, haciéndoles creer que interactúan con la página oficial del hotel, lo que podría llevar a realizar reservas o pagos fraudulentos.

Impacto en la seguridad del hotel:

- Fraude en reservas: Los visitantes pueden realizar reservas falsas en sitios web fraudulentos, generando pérdidas económicas para el hotel.
- Robo de información: Los atacantes pueden capturar información personal y financiera de los usuarios que creen estar utilizando la página legítima del hotel.
- Daño a la reputación: La presencia de sitios web falsos puede afectar la confianza de los clientes y dañar la reputación del hotel.
- Pérdida de ingresos: La realización de pagos fraudulentos y reservas no legítimas puede resultar en pérdida de ingresos para el hotel.

1.1.10 Ataques a sistemas POS

Los ataques a sistemas Punto de Venta (POS) se enfocan en comprometer la seguridad de los puntos de venta utilizados para procesar transacciones de pago, como las ubicadas en recepciones, restaurantes y tiendas dentro del hotel. Estos ataques buscan obtener acceso no autorizado a la información financiera de los huéspedes y clientes que realizan transacciones en estos puntos.

Modo de operación:

- Infiltración: Los atacantes buscan infiltrarse en el sistema POS, ya sea mediante malware, exploits o técnicas de ingeniería social.
- Exfiltración de datos: Una vez comprometido, el atacante intenta exfiltrar datos de transacciones financieras, incluyendo información de tarjetas de crédito y datos personales.
- Uso de datos robados: La información robada puede utilizarse para realizar transacciones fraudulentas o venderse en el mercado negro.

Impacto en la seguridad del hotel:

- Fraude financiero: Los datos comprometidos pueden ser utilizados para realizar transacciones fraudulentas, generando pérdidas financieras para el hotel y los clientes.
- Pérdida de confianza: La revelación de información financiera sensible puede afectar la confianza de los clientes en la seguridad del hotel.
- Cumplimiento normativo: La pérdida de datos financieros puede tener implicaciones legales y regulatorias, especialmente en relación con normativas como PCI DSS.

El grupo Play reclama el ataque a la cadena hotelera alemana H-Hotels

El pasado diciembre, la cadena hotelera H-Hotels, una reconocida empresa hotelera que opera 60 hoteles en 50 ubicaciones en Alemania, Austria, Suiza, Francia y Hungría, fue objeto de un ciberataque que provocó interrupciones en los sistemas de comunicación de la empresa.

Aunque el ataque no afectó las reservas de los huéspedes, según el aviso del incidente de seguridad de la compañía, "los ciber delincuentes lograron vulnerar los amplios sistemas de protección técnica y organizativa en un ataque profesional". En respuesta al ataque, los sistemas se cerraron inmediatamente y se desconectaron de internet.

Play *ransomware* Se atribuyó el ataque y añadió a la compañía su sitio Tor, afirmando haber robado una gran cantidad de datos. Sin embargo, no llegaron a publicar ninguna muestra de dichos datos.

Play es un grupo prorruso, que distribuye el malware playcrypt, un ransomware que afecta a sistemas Windows y que apareció por primera vez en julio de 2022.

Un grupo de hackers accede a las bases de datos de la cadena hotelera InterContinental Hotels gracias a la contraseña Qwerty1234

Uno de los mayores grupos hoteleros del mundo, que cuenta con más de 6.000 hoteles en un centenar de países, IHG (InterContinental Hotels Group), fue víctima en septiembre de 2022 de un ciberataque que causó la caída de su red interna durante más de 24 horas. Fueron los propios clientes los que alertaron de que algo ocurría, ya que muchos informaron de problemas generalizados con las reservas y check-ins en su plataforma. Durante 24 horas IHG afirmó que la empresa estaba "en mantenimiento del sistema", aunque al día siguiente confirmó que había sufrido un cibertaque.

Todo comenzó con un email de *phishing* que logró engañar a un empleado de la compañía para que descargara un *malware* adjunto, que capturaba su código de autenticación de doble factor. A continuación, consiguieron acceder al gestor de contraseñas con la clave 'Qwerty1234', una de las más frecuentes, y, por tanto, inseguras del mundo.

El grupo intentó implantar un *ransomware* que cifrara los datos de la compañía, pero la empresa consiguió proteger sus servidores a tiempo. Al ser frustrado su intento de *ransomware*, realizaron un ataque de tipo *Wiper*, eliminando de forma irreversible datos sensibles de la compañía. Aunque no consiguieron robar una importante cantidad de datos, sí obtuvieron datos corporativos y algunos registros de correo electrónico.

1.2 Vectores de ataque

La seguridad cibernética en la industria hotelera se ve constantemente desafiada por diversos vectores de ataque que buscan explotar vulnerabilidades en la infraestructura, sistemas y prácticas operativas. La comprensión y mitigación efectiva de estos vectores son esenciales para salvaguardar la integridad de los datos y garantizar la continuidad operativa.

A continuación, se detallan algunos de los principales vectores de ataque y estrategias de mitigación asociadas:

1.2.1 Redes no segmentadas

La carencia de segmentación entre las redes del hotel representa una significativa vulnerabilidad, ya que permite a un potencial atacante desplazarse sin restricciones dentro de la infraestructura. Esta falta de aislamiento posibilita el acceso indiscriminado a sistemas críticos y datos sensibles de los clientes. La consecuencia directa puede ser la comprometida integridad de los sistemas de gestión hotelera, impactando negativamente en la operación del establecimiento y, por ende, en la satisfacción del cliente.

Estrategias de mitigación efectivas:

- Segmentación lógica de redes: Establecimiento de segmentos lógicos en la red del hotel para la división de áreas funcionales, tales como administración, reservas y servicios al cliente. Este enfoque limita el acceso a sistemas críticos según la necesidad.
- Firewalls y políticas de acceso: Implementación de firewalls robustos para el control del tráfico entre segmentos de red y la definición de políticas de acceso estrictas. Esto garantiza que únicamente usuarios autorizados tengan acceso a áreas específicas.
- Autenticación de usuarios: Refuerzo de los mecanismos de autenticación para asegurar que sólo el personal autorizado tenga acceso a segmentos de red específicos. La implementación de autenticaciones multifactoriales agrega una capa adicional de seguridad.
- Monitorización continua: Establecimiento de un sistema de monitorización continua que supervise la actividad de red y detecte cualquier intento de movimiento no autorizado entre segmentos. Las alertas tempranas permiten una respuesta rápida en caso de incidente.

1.2.2 Falta de concienciación

La falta de concienciación entre el personal hotelero en relación con las mejores prácticas de ciberseguridad constituye un riesgo sustancial. La carencia de conocimientos puede exponer al hotel a ataques de ingeniería social, malas prácticas de seguridad y deficiencias en la detección o respuesta a incidentes cibernéticos. Para abordar este desafío, se vuelve imperativa la implementación de programas educativos y de concienciación con el objetivo de fortalecer la resiliencia del hotel ante amenazas digitales.

Estrategias de mitigación efectivas:

- Programas de formación continua: Establecimiento de programas de formación regulares para el personal hotelero, abordando temas clave de ciberseguridad, incluyendo la identificación de amenazas, prácticas seguras de navegación y la importancia de la seguridad de la información.
- Simulacros de phishing: Realización de simulacros de phishing para evaluar la capacidad del personal para reconocer correos electrónicos fraudulentos. Estos ejercicios prácticos permiten mejorar la conciencia y la capacidad de respuesta ante posibles intentos de ingeniería social.
- Políticas de uso de dispositivos personales: Desarrollo de políticas claras sobre el uso de dispositivos personales en entornos laborales. La concienciación sobre los riesgos asociados con dispositivos no seguros contribuye a la prevención de amenazas.
- Sensibilización sobre contraseñas seguras: Campañas informativas sobre la importancia de contraseñas seguras y su gestión adecuada. Se promueve el uso de contraseñas robustas y se fomenta el cambio periódico de las mismas.

1.2.3 Falta de seguridad en dispositivos

La falta de medidas de seguridad efectivas en dispositivos, ya sean propiedad de la organización o de uso personal (BYOD), representa un riesgo significativo al aumentar la superficie de ataque. Vulnerabilidades no parcheadas, configuraciones inseguras o la instalación de software no seguro contribuyen a una exposición mayor a amenazas cibernéticas. Para abordar este desafío, es imperativo implementar políticas robustas de seguridad con el objetivo de mitigar estos riesgos.

Estrategias de mitigación efectivas:

- Gestión de parches y actualizaciones: Establecimiento de un proceso formal para la gestión de parches y actualizaciones en todos los dispositivos. Garantizar que todos los sistemas estén al día con las últimas correcciones de seguridad.
- Políticas de BYOD claras: Desarrollo de políticas claras para dispositivos de uso personal que acceden a la red del hotel. Especificar requisitos mínimos de seguridad y configuraciones permitidas.
- Herramientas de seguridad en dispositivos: Implementación de soluciones de seguridad, como antivirus y antimalware, en todos los dispositivos. Estas herramientas ayudan a detectar y mitigar posibles amenazas.
- Encriptación de dispositivos móviles: Requerir la encriptación de dispositivos móviles que acceden a la red del hotel. La encriptación protege la información sensible en caso de pérdida o robo.
- Autenticación fuerte en dispositivos: Promover el uso de métodos de autenticación fuerte, como autenticación multifactorial, en todos los dispositivos. Esto añade una capa adicional de seguridad.

1.2.4 Sistemas desactualizados

La utilización de software obsoleto y sistemas heredados en el entorno hotelero introduce potenciales puntos de vulnerabilidad. Las versiones de software no compatibles pueden carecer de los parches de seguridad cruciales, lo que las hace susceptibles a la explotación por parte de adversarios cibernéticos. Para abordar este desafío, es esencial implementar estrategias de mitigación que aseguren la seguridad cibernética de manera efectiva.

Estrategias de mitigación efectivas:

- Inventario de sistemas y software: Realización de un inventario exhaustivo de todos los sistemas y software utilizados en el entorno hotelero. Esto incluye sistemas operativos, aplicaciones y cualquier componente de red.
- Políticas de actualización regular: Establecimiento de políticas formales que requieran la actualización regular de todos los sistemas y software. Definir un calendario de actualizaciones para garantizar la aplicación oportuna de parches de seguridad.
- Automatización de actualizaciones: Implementación de herramientas de automatización para gestionar y aplicar actualizaciones de manera eficiente. La automatización reduce el riesgo de omisiones humanas y garantiza una cobertura completa.
- Evaluación de compatibilidad: Antes de realizar actualizaciones, llevar a cabo evaluaciones de compatibilidad para asegurar que las nuevas versiones de software sean adecuadas para el entorno hotelero y no generen conflictos.

1.2.5 Malas prácticas

La adopción de malas prácticas en el entorno hotelero, tales como contraseñas débiles, el uso compartido de credenciales, redes Wi-Fi poco seguras y la falta de cifrado de datos confidenciales, incluyendo la información de huéspedes y detalles de pago, amplía las vulnerabilidades y compromete la seguridad cibernética.

Estrategias de mitigación efectivas:

- Políticas de contraseñas robustas: Establecimiento de políticas que requieran contraseñas robustas, combinando caracteres alfanuméricos, símbolos y letras mayúsculas y minúsculas. Fomentar la actualización regular de contraseñas.
- Autenticación multifactorial: Implementación de autenticación multifactorial para agregar una capa adicional de seguridad. Esto requiere la verificación de identidad a través de múltiples métodos, como contraseñas y códigos de acceso temporal.

Brecha de seguridad en Choice Hotels por una vulnerabilidad en MOVEit Transfer

Choice Hotels International, la empresa propietaria de Radisson Hotels, confirmó en julio de 2023 que los datos de los huéspedes de la cadena hotelera se vieron comprometidos. Choice Hotels es una de las cadenas hoteleras más grandes del mundo, que cuenta con varias marcas de hoteles.

La brecha de datos fue producida por una vulnerabilidad en MOVEit Transfer, explotada por la banda de ransomware Cl0p, y descubierta 20 días después de que ocurriera. Uno de los proveedores de Choice Hotels contaba con el software MOVEit, lo que resultó en las filtraciones de datos que afectaron a muchos de sus clientes, incluido Radisson Hotels Americas. MOVEit es un producto de software de transferencia de archivos administrado por terceros, utilizado por las principales empresas de los sectores energético, financiero, minorista y legal, así como por el sector hotelero.

Una supuesta violación de datos de Airbnb expone 1,2 millones de registros de usuarios

Una filtración de datos habría comprometido la seguridad de Airbnb, exponiendo potencialmente la información personal de 1,2 millones de usuarios a finales de octubre de 2023.

El atacante, conocido como "Sheriff" en la Dark Web, y del que no hay mucha información, reclamó la filtración, fijando un precio inicial de 7.000 dólares por la venta ilícita de estos datos. La disponibilidad de dichos datos en el mercado negro plantea serias preocupaciones sobre la seguridad y privacidad de los datos de usuarios de Airbnb.

No es la primera vez que la compañía se enfrenta a problemas relacionados con la ciberseguridad. En agosto de 2023, la Comisión Irlandesa de Protección de Datos se enfrentó a Airbnb Irlanda por infracciones relacionadas con la conservación y el procesamiento de documentos de identidad.

Hostelería, el tercer gremio del sector servicios que más ciberataques sufre

La hostelería es el tercer gremio más afectado del sector servicios, después de las tecnológicas y consultorías. Al menos un 18% ha sufrido algún ataque en el último año y se estima que un 40% no logra recuperarse del ataque. Los tipos de ataque más frecuente son el ransomware, malware y el phishing.

Los ciberataques más habituales en hoteles en 2023

- **Spearphishing.** Los atacantes estudian a la víctima, obtienen el correo electrónico de reservas del hotel y suplantan la identidad para cobrar en cuentas propias.
- **Clonado de Webs Hoteleras.** Replican la web de un hotel, engañando a las víctimas para realizar pagos sin detectar la falsificación.
- **Códigos QR**: Se crean códigos falsos para infectar dispositivos de clientes al acceder a webs maliciosas.
- **Acceso a Redes No Segmentadas**. La falta de segmentación en las redes Wifi facilita el acceso no autorizado, permitiendo a los atacantes obtener datos sensibles de la empresa.
- **Insiders y Clientes Comprometidos**: Trabajadores insatisfechos o con dispositivos comprometidos pueden realizar ataques internos, vendiendo información o servicios a terceros.
- **Explotación de la Falta de Seguridad en Dispositivos personales**: El uso creciente de dispositivos personales en entornos laborales aumenta los riesgos de seguridad, incluyendo la instalación de software no seguro.
- **Ataques en la Cadena de Suministro**. La descentralización en la hostelería permite a los atacantes obtener información a través de intermediarios, comprometiendo la cadena de suministro y afectando a la resiliencia de los servicios.

- Educación continua del personal: Realización de programas educativos continuos para concienciar al personal sobre la importancia de prácticas seguras. Esto incluye la promoción de contraseñas únicas y el reconocimiento de posibles ataques.
- Redes Wi-Fi seguras: Configuración de redes Wi-Fi seguras mediante la implementación de cifrado WPA3, contraseñas fuertes y segmentación de red para separar tráfico crítico del público.

1.2.6 Falta de monitorización y respuesta ante incidentes

La ausencia de un plan de respuesta a incidentes bien definido deja al hotel vulnerable a consecuencias graves en caso de violaciones de seguridad. Sin una monitorización eficaz y procesos de respuesta claros, los retrasos en la identificación y mitigación de amenazas pueden agravar el impacto de un incidente de seguridad. La implementación de sistemas de monitorización proactiva y protocolos de respuesta robustos es esencial para la defensa contra amenazas emergentes.

Estrategias de mitigación efectivas:

- Implementación de sistemas de monitorización proactiva: Despliegue de sistemas avanzados de monitorización que detecten de manera proactiva anomalías y actividades sospechosas en la red. La monitorización constante permite una identificación temprana de posibles amenazas.
- Definición de protocolos de respuesta: Establecimiento de protocolos de respuesta claros y bien documentados para cada tipo de incidente de seguridad. Esto incluye pasos específicos a seguir desde la detección hasta la resolución.
- Entrenamiento del personal en respuesta a incidentes: Capacitación regular del personal en los procedimientos de respuesta a incidentes. Un equipo preparado puede actuar de manera rápida y eficiente ante amenazas, minimizando el impacto.
- Simulacros de incidentes: Realización periódica de simulacros de incidentes para poner a prueba la eficacia de los protocolos de respuesta. Los simulacros ayudan a identificar áreas de mejora y garantizan una respuesta efectiva en situaciones reales.
- Automatización de la respuesta: Implementación de herramientas de automatización para respuestas rápidas ante amenazas comunes. La automatización reduce el tiempo de respuesta y minimiza el riesgo de errores humanos.

2. Normativa y sanciones en materia de ciberseguridad aplicables al sector

En un entorno hotelero cada vez más digitalizado, la gestión de datos personales de los huéspedes se ha convertido en un componente esencial de la operación diaria. La introducción de tecnologías innovadoras ha ampliado la superficie de ataque cibernético, haciendo que la protección efectiva de los datos sea una prioridad crítica para los establecimientos y sus equipos de tecnologías de la información (IT). En este contexto, la adhesión a normativas específicas se torna imperativa, no solo para el cumplimiento legal, sino también para garantizar la confianza del cliente y preservar la reputación del establecimiento.

Las normativas que regulan la protección de datos en hoteles incluyen:

Reglamento General de Protección de Datos (RGDP)

El RGPD es una legislación clave que establece directrices para el tratamiento de datos personales de los ciudadanos de la Unión Europea (UE). Es crucial para cualquier organización, incluidos los hoteles, que procesa datos personales de residentes de la UE.

- **Aplicación:**

  A nivel europeo.

- **Principales aspectos:**

  - Consentimiento explícito: Se requiere un consentimiento claro y específico para el procesamiento de datos personales, asegurando que los individuos estén completamente informados y consientan de manera consciente y voluntaria.
  - Derechos ampliados: Los derechos de los individuos incluyen la portabilidad de datos y la limitación del procesamiento. Esto garantiza que las personas tengan un control más amplio sobre sus datos personales.

- **Implicaciones para SOC Hotelero:**

  - Evaluación del Impacto de Privacidad (PIA):
    - ✓ Requisito RGPD: Las organizaciones, incluidos los SOCs hoteleros, deben realizar Evaluaciones del Impacto de Privacidad (PIAs) para identificar y abordar los riesgos para la privacidad asociados con el procesamiento de datos.
    - ✓ Enfoque proactivo: Implica un enfoque proactivo para evaluar y mitigar los riesgos antes de llevar a cabo ciertas operaciones de procesamiento.
  - Derechos ampliados:
    - ✓ Implementación práctica: El SOC debe asegurar la implementación efectiva de los derechos ampliados otorgados por el RGPD. Esto incluye establecer procesos para garantizar la portabilidad de datos y abordar las solicitudes de limitación del procesamiento.
    - ✓ Transparencia y control: Es fundamental proporcionar transparencia a los individuos sobre cómo se procesan sus datos y ofrecerles control sobre su información personal.
  - Enfoque orientado a seguridad por diseño y gestión del riesgo:
    - ✓ Contribución del SOC a la mitigación de los riesgos mediante estrategias de monitorización y alerta temprana.

- **Consideraciones adicionales:**

  - Registro de actividades de tratamiento: El RGPD exige que las organizaciones, incluidos los hoteles, mantengan registros detallados de sus actividades de procesamiento de datos.
  - Notificación de brechas de seguridad: En caso de una violación de seguridad que pueda afectar los derechos y libertades de los individuos, se requiere informar a la autoridad de supervisión y a los propios individuos.
  - Designación de un Delegado de Protección de Datos (DPD): En ciertos casos, se debe designar un DPD para supervisar el cumplimiento del RGPD, especialmente en organizaciones que realizan un gran volumen de procesamiento de datos.

- **Enfoque integral:**

  - El RGPD no solo establece estándares para garantizar la privacidad de los datos, sino que también promueve una cultura de protección de la privacidad. Requiere una gestión cuidadosa de los datos personales y un enfoque proactivo para garantizar el cumplimiento continuo. La cooperación activa con las autoridades de protección de datos y la atención constante a los derechos de los individuos son esenciales para cumplir con los requisitos del RGPD.

Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)

La LOPDGDD es la legislación española que adapta y complementa el Reglamento General de Protección de Datos (RGPD) a nivel nacional. Su aplicación tiene un alcance específico en el marco legal español y aborda aspectos adicionales que no están cubiertos de manera exhaustiva por el RGPD.

- **Aplicación:**

  Marco legal español que adapta y complementa el RGDP.

- **Principales aspectos:**

  - Registro de actividades de tratamiento: Obligación de mantener un registro de las operaciones de procesamiento de datos ya que es una herramienta fundamental para garantizar la transparencia y el cumplimiento.
  - Menores de edad: Regula el tratamiento de datos de menores de 14 años, estableciendo la necesidad de obtener el consentimiento de los padres o tutores para el procesamiento de datos de estos menores. Reconoce la importancia de la protección de la privacidad de los menores y establece medidas adicionales para garantizar un tratamiento adecuado de sus datos.

- **Implicaciones para SOC Hotelero:**

  - Implementación de medidas de seguridad:
    - ✓ Requisitos técnicos y organizativos: El SOC hotelero debe establecer medidas técnicas y organizativas sólidas para garantizar la seguridad de los datos personales. Esto incluye controles de acceso, cifrado de datos, y otras prácticas de seguridad informática.
    - ✓ Adaptación a la evolución tecnológica: Dado que la tecnología y las amenazas evolucionan, el SOC debe adaptar continuamente sus medidas de seguridad para hacer frente a los riesgos emergentes.
    - ✓ Monitorización de los casos de uso relacionados con los principales riesgos a los que está expuesta la organización.

  - Notificación de violaciones de seguridad:
    - ✓ Obligación de informar: La LOPDGDD obliga a informar a la Agencia Española de Protección de Datos (AEPD) y a los afectados en caso de violaciones de seguridad que puedan comprometer la privacidad de los datos.
    - ✓ Rapidez y eficiencia: El SOC debe contar con procedimientos rápidos y eficientes para detectar, evaluar y notificar las violaciones de seguridad, minimizando así el impacto en los individuos afectados.

- **Consideraciones adicionales:**

  - Evaluación de Impacto en la Protección de Datos (EIPD): En ciertos casos, la LOPDGDD puede requerir la realización de Evaluaciones de Impacto en la Protección de Datos para evaluar los riesgos asociados con operaciones específicas de procesamiento de datos.
  - Delegado de Protección de Datos (DPD): Similar al RGPD, la LOPDGDD puede requerir la designación de un DPD en ciertos escenarios.

- **Enfoque integral:**

  - El cumplimiento con la LOPDGDD implica un enfoque integral hacia la protección de datos, desde la documentación y registro adecuado hasta la implementación de medidas de seguridad y la notificación eficiente de violaciones. La adaptación constante a los requisitos legales y la colaboración con la AEPD son esenciales para asegurar un alto nivel de cumplimiento.

Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI-CE)

La LSSI-CE es una ley española que regula los servicios de la sociedad de la información y el comercio electrónico en España.

- **Aplicación:**

Regula servicios y comercio electrónico en España.

- **Principales aspectos:**

  - Conservación de documentación electrónica: Establece requisitos específicos para la conservación de documentos electrónicos relacionados con transacciones comerciales realizadas a través de servicios de la sociedad de la información y plataformas de comercio electrónico. Estos requisitos buscan asegurar la integridad y disponibilidad de la documentación electrónica, garantizando la confianza en las transacciones digitales.

- **Infracciones:**

  La LSSI-CE clasifica las infracciones en tres categorías con multas asociadas:
  - Muy grave → Multa de 150.001 a 600.000 euros
  - Grave → Multa de 30.001 s 150.000 euros
  - Leve → Multa de hasta 30.000 euros.

- **Implicaciones para SOC Hotelero:**

  - Seguridad en plataformas digitales: El SOC en un entorno hotelero debe implementar medidas de seguridad robustas en las plataformas digitales utilizadas para ofrecer servicios de comercio electrónico, como reservas en línea, servicios adicionales, etc. La seguridad en estas plataformas es esencial para proteger la integridad de la información transaccional, salvaguardar la privacidad de los usuarios y garantizar la continuidad operativa.
  - Gestión de incidentes: Desarrollar planes y procedimientos para la gestión de incidentes relacionados con la seguridad de la información en plataformas digitales. Responder de manera eficiente a posibles brechas de seguridad y violaciones, minimizando el impacto en los clientes y en la reputación del hotel.
  - Cumplimiento normativo: Asegurar que las plataformas digitales cumplan con los requisitos de conservación de documentación electrónica establecidos por la LSSI-CE. Implementar controles para la correcta gestión y almacenamiento de la documentación relacionada con transacciones electrónicas.

- **Consideraciones adicionales:**

  - Gestión de la privacidad: El SOC debe colaborar estrechamente con el equipo de privacidad para garantizar que las prácticas de seguridad en las plataformas digitales cumplan con los estándares de privacidad definidos por la LSSI-CE. Esto incluye la protección de datos sensibles y la gestión adecuada del consentimiento del usuario.
  - Capacitación y concientización: Implementar programas de capacitación para el personal del hotel sobre las obligaciones y responsabilidades establecidas por la LSSI-CE. Esto ayuda a crear una cultura de seguridad informática y a reducir el riesgo de errores humanos que puedan resultar en infracciones.
  - Monitoreo continuo: Establecer sistemas de monitoreo continuo en las plataformas digitales para detectar y responder rápidamente a posibles amenazas de seguridad. Esto incluye la monitorización de accesos no autorizados, actividad sospechosa y posibles violaciones de la LSSI-CE.
  - Documentación y auditoría interna: Mantener una documentación exhaustiva de los procesos de seguridad implementados y realizar auditorías internas periódicas para evaluar la efectividad de los controles. Esto ayuda a identificar áreas de mejora y garantiza un enfoque proactivo hacia la seguridad.
  - Notificación de violaciones: Desarrollar un proceso claro y eficiente para notificar violaciones de seguridad a la Agencia Española de Protección de Datos (AEPD) y a los afectados, cumpliendo con los requisitos de la LSSI-CE. La rapidez y precisión en la notificación son fundamentales.

- **Enfoque integral:**

  - El cumplimiento integral de la LSSI-CE implica una combinación de medidas técnicas, organizativas y legales para garantizar la seguridad, privacidad y conformidad en las operaciones digitales y de comercio electrónico. Un enfoque proactivo y colaborativo es esencial para enfrentar los desafíos en un entorno digital en constante cambio.

Directiva Europea 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 (PSD2)

La Directiva Europea 2015/2366 del Parlamento Europeo y del Consejo, conocida como PSD2 y promulgada el 25 de noviembre de 2015, tiene un impacto significativo en los servicios de pago en la Unión Europea. La PSD2 regula de manera específica los servicios de pago en la Unión Europea, estableciendo normativas para garantizar la seguridad y la innovación en las transacciones financieras.

- **Aplicación:**

  Regula los servicios de pago en el mercado interior de la Unión Europea.

- **Principales aspectos:**

  - Autenticación reforzada del cliente (SCA): Requiere medidas adicionales para verificar la identidad del cliente en transacciones electrónicas.
  - Acceso a datos de cuentas: Permite la apertura de cuentas de pago a terceros.

- **Infracciones:**

  - Leves → Multa de hasta el 1% del importe neto anual de la cifra de negocios
  - Graves → Multa de hasta el 5% del importe neto anual de la cifra de negocios más una amonestación pública.

- **Implicaciones para SOC Hotelero:**

  - Seguridad en transacciones financieras: Implementación de medidas robustas para garantizar la autenticación y seguridad en las transacciones financieras. Se deben desarrollar e implementar tecnologías y controles de seguridad avanzados para salvaguardar la integridad de las transacciones financieras, minimizando riesgos de fraude y asegurando la confianza de los clientes en los servicios financieros del hotel. La monitorización por parte del SOC hotelero de los casos de uso relacionados con la autenticación y con las interfaces entre las diferentes partes conectadas, son clave en esa protección.

- **Consideraciones adicionales:**
  - Gestión de incidentes financieros:
    - ✓ Establecimiento de protocolos: Desarrollar protocolos claros para la gestión de incidentes financieros, respondiendo rápidamente a posibles amenazas y minimizando el impacto en la operación del hotel.
  - Capacitación continua del personal:
    - ✓ Programas de formación: Implementar programas de capacitación continua para el personal, asegurando un alto nivel de conciencia sobre las últimas amenazas y mejores prácticas en seguridad financiera.

- **Enfoque integral:**
  - El cumplimiento integral de la PSD2 implica, por lo tanto, una combinación de medidas técnicas, operativas y legales para garantizar la seguridad y la confianza en las transacciones financieras electrónicas, así como para fomentar la innovación y la competencia en el sector de servicios de pago.

Real Decreto-ley 19/2018, de 23 de noviembre

Este Real Decreto-ley, en vigor desde el 24 de noviembre de 2018, se centra en regulares aspectos relacionados con servicios de pago y otras medidas urgentes en el ámbito financiero en España. Su aplicación abarca un amplio espectro de actividades financieras, con el objetivo de fortalecer la seguridad y eficiencia en las transacciones.

- **Aplicación:**

  Se centra en servicios de pago y otras medidas urgentes en materia financiera.

- **Principales aspectos:**

  Limitación de responsabilidad del usuario: Este decreto establece normativas específicas que definen la responsabilidad del usuario en situaciones de pérdida o robo de instrumentos de pago. Establece límites claros para la responsabilidad financiera del titular del instrumento de pago, brindando seguridad jurídica en casos de eventos adversos.

- **Infracciones:**
  - Leves → Multa de hasta el 1% del importe neto anual de la cifra de negocios
  - Graves → Multa de hasta el 5% del importe neto anual de la cifra de negocios más una amonestación pública.

- **Implicaciones para SOC Hotelero:**
  - Protección de información financiera: Se deben implementar medidas de seguridad para proteger la información financiera de los huéspedes durante las transacciones. También una adopción de tecnologías y prácticas de seguridad actualizadas para prevenir accesos no autorizados y garantizar la confidencialidad de los datos financieros. La monitorización por parte del SOC hotelero de los casos de uso relacionados son clave en esa protección.

- **Consideraciones adicionales:**
  - Gestión de riesgos financieros: Desarrollo de estrategias proactivas para la identificación y mitigación de riesgos financieros, considerando posibles amenazas y vulnerabilidades en las operaciones de pago.
  - Colaboración con proveedores de servicios de pago: Colaboración continua con proveedores de servicios de pago para asegurar que las medidas de seguridad implementadas sean consistentes con las mejores prácticas y regulaciones vigentes.
  - Monitoreo continuo: Establecimiento de sistemas de monitoreo continuo para detectar y responder de manera inmediata a cualquier incidente que pueda comprometer la seguridad financiera.

- **Enfoque integral:**
  - El cumplimiento integral de este Real Decreto-ley requiere un enfoque integral que no solo abarque aspectos técnicos, sino también estratégicos y operativos. La gestión efectiva de riesgos, la colaboración activa con los actores relevantes y el mantenimiento de prácticas de seguridad actualizadas son esenciales para garantizar la conformidad con la normativa y la protección de los datos financieros en el entorno hotelero.

PCI – Payment Card Industry – Estándar de Seguridad de Datos.

El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) es un marco global que se aplica a nivel mundial, especialmente diseñado para la industria de tarjetas de pago. Su objetivo es establecer medidas de seguridad robustas y garantizar la protección de la información confidencial asociada con transacciones con tarjetas de pago.

- **Aplicación:**

  A nivel global, enfocado en la industria de tarjetas de pago.

- **Principales aspectos:**

  - Protección de datos de tarjetas de pago:
    - ✓ PDI DSS establece normas estrictas para garantizar la privacidad y seguridad de la información de tarjetas de pago.
    - ✓ Incluye medidas para el almacenamiento, transmisión y procesamiento seguro de estos datos.
  - Control de acceso:
    - ✓ Requiere la implementación de controles de acceso sólidos para restringir el acceso a datos confidenciales de tarjetas de pago.
    - ✓ Autenticación multifactor y restricciones de acceso basada en roles.

- **Implicaciones para SOC Hotelero:**

  - PCI DSS impone requisitos específicos para que los establecimientos hoteleros implementen medidas de seguridad destinadas a proteger las transacciones financieras que involucran tarjetas de pago.
  - Adopción de controles rigurosos: Los hoteles deben adoptar controles rigurosos, como cifrado de datos, firewalls, y políticas de acceso, para cumplir con las normativas de PCI DSS. La efectividad de estos controles debe ser monitorizada.
  - Auditorías periódicas: Es crucial realizar auditorías periódicas para evaluar y verificar el cumplimiento continuo de estas normativas de seguridad. El SOC hotelero debe tener en especial consideración las vulnerabilidades resultantes de estas auditorías, estableciendo medidas compensatorias de monitorización y colaborando en la resolución de dichas vulnerabilidades.
  - Creación de casos de uso específicos de monitorización para la protección de la integridad de las operaciones financieras: El cumplimiento exitoso asegura la integridad de las operaciones financieras del hotel, generando confianza tanto en los huéspedes como en las entidades financieras.

- **Consideraciones adicionales:**

  - Formación del personal: Implementar programas de formación para el personal del hotel sobre las mejores prácticas de seguridad establecidas por PCI DSS.
  - Gestión de incidentes: Desarrollar planes y procedimientos de gestión de incidentes para responder rápidamente a posibles brechas de seguridad, integración de las capacidades del SOC hotelero con la organización.
  - Colaboración con proveedores: Colaborar estrechamente con proveedores de servicios de pago para garantizar la coherencia en la aplicación de medidas de seguridad y su posible integración en el SOC hotelero.

- **Enfoque integral:**

  - El cumplimiento integral con PCI DSS exige un enfoque holístico que abarque desde la formación del personal hasta la implementación de tecnologías avanzadas, asegurando la continua adaptación a las mejores prácticas de seguridad en la industria de tarjetas de pago. Esto contribuye a un entorno financiero seguro y confiable en el sector hotelero.

3. Recursos de ciberseguridad

La ciberseguridad:

- Glosario de términos de ciberseguridad: una guía de aproximación para el empresario: https://www.incibe.es/empresas/guias/glosario-de-terminos-de-ciberseguridad-una-guia-de-aproximacion-para-el
- Ciberseguridad en el sector turismo y ocio. Guía de recomendaciones para empresas: https://www.incibe.es/empresas/guias/ciberseguridad-el-sector-turismo-y-ocio-guia-recomendaciones-empresas

Tipos de ciberataques:

- Ransomware: una guía de aproximación para el empresario: https://www.incibe.es/empresas/guias/ransomware-guia-aproximacion-el-empresario
- Ciberamenazas contra entornos empresariales: una guía de aproximación para el empresario: https://www.incibe.es/empresas/guias/ciberamenazas-entornos-empresariales-guia-aproximacion-el-empresario
- ENISA Threat Landscape 2023 - European Union: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Buenas prácticas en materia de ciberseguridad:

- Principios y recomendaciones básicas en Ciberseguridad: https://www.ccn-cert.cni.es/es/informes/informes-de-buenas-practicas-bp/2473-ccn-cert-bp-01-principios-y-recomendaciones-basicas-en-ciberseguridad/file?format=html
- Buenas prácticas en el área de informática: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_buenas_practicas_en_el_area_de_informatica.pdf
- Seguridad en redes wifi: una guía de aproximación para el empresario: https://www.incibe.es/empresas/guias/seguridad-redes-wifi-guia-aproximacion-el-empresario
- Ciberseguridad en el teletrabajo: una guía de aproximación para el empresario: https://www.incibe.es/empresas/guias/ciberseguridad-en-el-teletrabajo-una-guia-de-aproximacion-para-el-empresario
- Seguridad en la instalación y uso de dispositivos IoT: una guía de aproximación para el empresario: https://www.incibe.es/empresas/guias/seguridad-instalacion-y-uso-dispositivos-iot-guia-aproximacion-el
- Ciberseguridad en comercio electrónico. Guía de recomendaciones para empresas: https://www.incibe.es/empresas/guias/guia-ciberseguridad-comercio-electronico
- Copias de seguridad: una guía de aproximación para el empresario: https://www.incibe.es/empresas/guias/copias-seguridad-guia-aproximacion-el-empresario
- Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario: https://www.incibe.es/empresas/guias/dispositivos-moviles-personales-uso-profesional-byod-guia-aproximacion-el
- Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario: https://www.incibe.es/empresas/guias/ganar-en-competitividad-cumpliendo-el-rgpd-una-guia-de-aproximacion-para-el

Gestión de incidentes de seguridad:

- Guía nacional de notificación y gestión de ciberincidentes: https://www.incibe.es/incibe-cert/guias-y-estudios/guias/guia-nacional-de-notificacion-y-gestion-de-ciberincidentes
- Cómo gestionar una fuga de información. Una guía de aproximación al empresario: https://www.incibe.es/empresas/guias/guia-fuga-informacion

INSTITUTO TÉCNICO HOTELERO
C/ Orense, 32 28020 Madrid
Tel.: +34 902 110 784 Fax: +34 91 770 19 82
info@ithotelero.com

GMV
OFICINAS CENTRALES
Isaac Newton 11 P.T.M. Tres Cantos - 28760 Madrid
Tel.: +34 91 807 21 00 Fax: +34 91 807 21 99