Ataques Cibernéticos en la Industria de la Hospitalidad

Enero, 2023

LOCKTON®

La Industria de la Hospitalidad es particularmente susceptible a los ciberataques debido a que enfrenta desafíos específicos que incrementan su vulnerabilidad, entre los que se encuentran: la rotación de personal, el aumento en el uso de los sistemas tecnológicos (reservaciones y pagos), grandes cantidades de datos (detalles de tarjetas bancarias), muchos dispositivos conectados y fallas en las políticas de seguridad, por mencionar algunos, es por ello que resulta imprescindible establecer una estrategia integral de ciberseguridad que permita proteger la operación, clientes, reputación e ingresos.

Si bien un ataque cibernético generalmente se dirige al Centro Operativo (recursos humanos, nómina, finanzas y sistemas de información) el daño potencial tiene un alcance mayúsculo debido a la gran cantidad de datos personales sensibles e información confidencial que se vulnera y que es valiosa en el "mercado negro".

Acceder a los datos de un hotel es como ganarse la lotería para los ciberatacantes. Una vez que ingresan, tienen acceso a números de tarjetas de crédito, información de pasaportes, detalles de vuelos e incluso acceso a algunos de los controles físicos del hotel (por el uso de IoT "Internet of Things" para el control de la luz, tarjetas de acceso a las habitaciones, TV´s, etc.) por lo que estar informados de las amenazas latentes es crucial.

Algunas ciber amenazas que enfrenta el sector son:

1. RANSOMWARE

Software malicioso diseñado para tomar información rehén que los ciberdelincuentes amenazan con publicar a menos que se pague un rescate o también llegando a bloquear el acceso a una red informática hasta que se pague dicho rescate.

2. ATAQUES DDoS (Distributed Denial-of-Service) o Ataque de denegación de servicio distribuido

Este tipo de ataques se basa en realizar solicitudes masivas de conexión a una dirección IP determinada, como un servidor, durante un cierto periodo de tiempo. Al recibir una enorme cantidad de peticiones simultáneamente, el servicio no puede dar respuesta a todas ellas y colapsa quedando fuera de servicio para los usuarios legítimos.

3. PHISHING (Suplantación de identidad)

Es la práctica de enviar correos electrónicos de un remitente de confianza que en realidad es de un cibercriminal. Algunos ejemplos son: el robo de datos de inicio de sesión para redirigir "phishees" a una página de inicio falsa y robar

información sensible, la liberación de malware (para pedir rescate) solicitando al destinatario que haga “clic” en un archivo adjunto o, cada vez más frecuente, haciéndose pasar por ejecutivos de empresas para autorizar pagos fraudulentos.

4. ATAQUES “DARKHOTEL”

Se caracteriza por hacer ataques dirigidos a altos ejecutivos en sus sitios de descanso mientras viajan. Consiste en tomar el control de las redes wifi de los hoteles de lujo, ahí los hackers desarrollan campañas de spear phishing muy detalladas y personalizadas para engañar a sus objetivos y robar información sensible.

5. ATAQUES A PUNTOS DE VENTA

El software malicioso se encuentra en dispositivos de punto de venta en restaurantes y bares dentro de cadenas hoteleras.

6. OTROS RIESGOS INCLUYEN:

A. Pérdidas financieras ante la gestión, remediación por violación de datos (incluido el incumplimiento normativo).

B. Las pérdidas por interrupción del negocio pueden acumularse rápidamente al actualizar los sistemas de reservación y las bases de datos.

C. Además, en la industria hipercompetitiva, el daño a la reputación es importante.

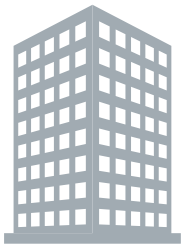
Algunos de los ataques informáticos más significativos en la industria han sido:

Cadena Hotelera Norteamericana

En el año 2015 se dio a conocer uno de los casos de ciberdelincuencia más mediáticos. Los equipos de punto de venta sufrieron una infección de malware. En total, 249 hoteles en más de 50 países se vieron afectados exponiendo la información privada de millones de clientes de todo el mundo.

Grupo Hotelero más grande de China

Sufrió un ataque cibernético a sus datos que afectó a más de 130 millones de personas. El atacante solicitó 60,000 dólares por devolver toda la información.



Hoteles Trump

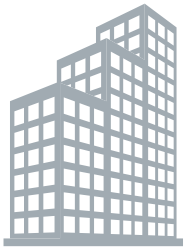
La cadena de hoteles del ex presidente de Estados Unidos, Donald Trump, fue hackeada entre el año 2015 y 2017. Hasta 14 de sus hoteles fueron víctimas del ciberataque, donde se hicieron con las tarjetas de créditos de los clientes e infectaron cientos de ordenadores y TPVs.

Hotel en Austria

Los turistas del lujoso hotel se quedaron sin poder acceder a sus habitaciones debido a un ciberataque con malware que afectó a los sistemas de llaves electrónicas.

Hotel en Orlando Florida (USA)

Los hackers estuvieron durante un año y medio obteniendo información de los clientes sin que la empresa hotelera tuviese constancia de ello. Millones de tarjetas de crédito fueron obtenidas por los cibercriminales, así como datos personales.



Grupo Hotelero de Gran Bretaña

Este 2022 la cadena confirmó haber tenido un ciberataque debido a que la contraseña de las bases de datos era de las más comunes y sencillas que se conocen. Los clientes de la cadena se quejaron de que las reservas y los check-in no funcionaban, por lo que la cadena debió responder quejas en redes sociales asegurando que había un “mantenimiento del sistema” con el riesgo reputacional que eso implica.

Administración del Riesgo Cibernético

Independientemente del tipo de exposición al que se haga frente, como parte de la estrategia de ciberseguridad, es importante llevar a cabo un proceso de administración que permita identificar, evaluar, mitigar o transferir el riesgo, siendo el Seguro Cibernético una gran herramienta de Transferencia.

Los Seguros Tradicionales de Propiedad, Responsabilidad Civil, entre otros, protegen los activos fijos de la compañía, y por supuesto, la vida y la salud de los empleados, pero frente a una "violación cibernética", la cobertura otorgada por el Seguro de Riesgo Cibernético es la solución.

¿Qué ampara el Seguro de Riesgo Cibernético?

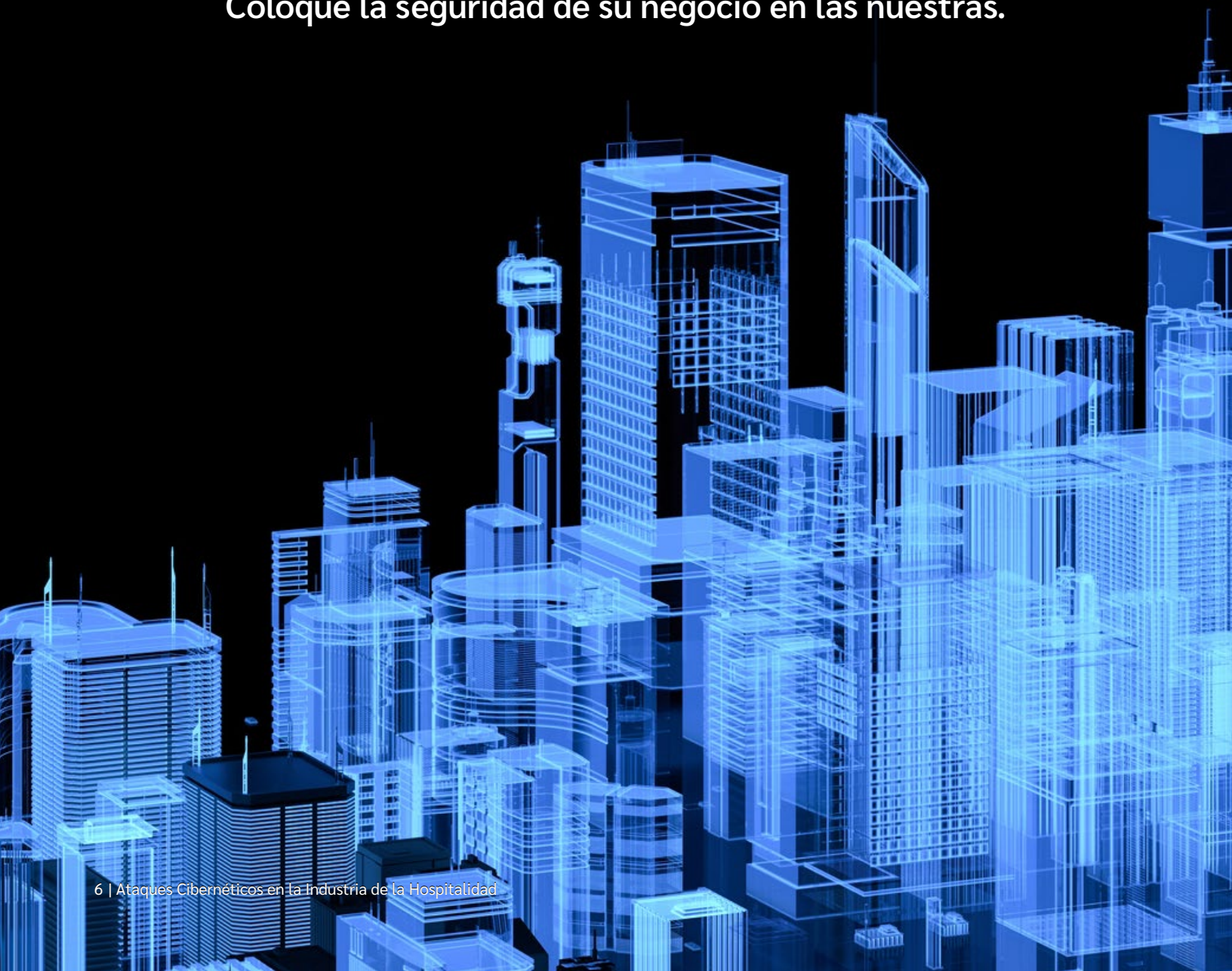
Protege a las empresas que tienen en su poder datos electrónicos y hacen uso de herramientas tecnológicas, contra los riesgos de: robo, pérdida, comunicación o divulgación de información no autorizada y que pueda causar daños. Estos daños pueden ser tanto a terceros como a sus propias operaciones incluido el pago de multas impuestas por parte de la autoridad.

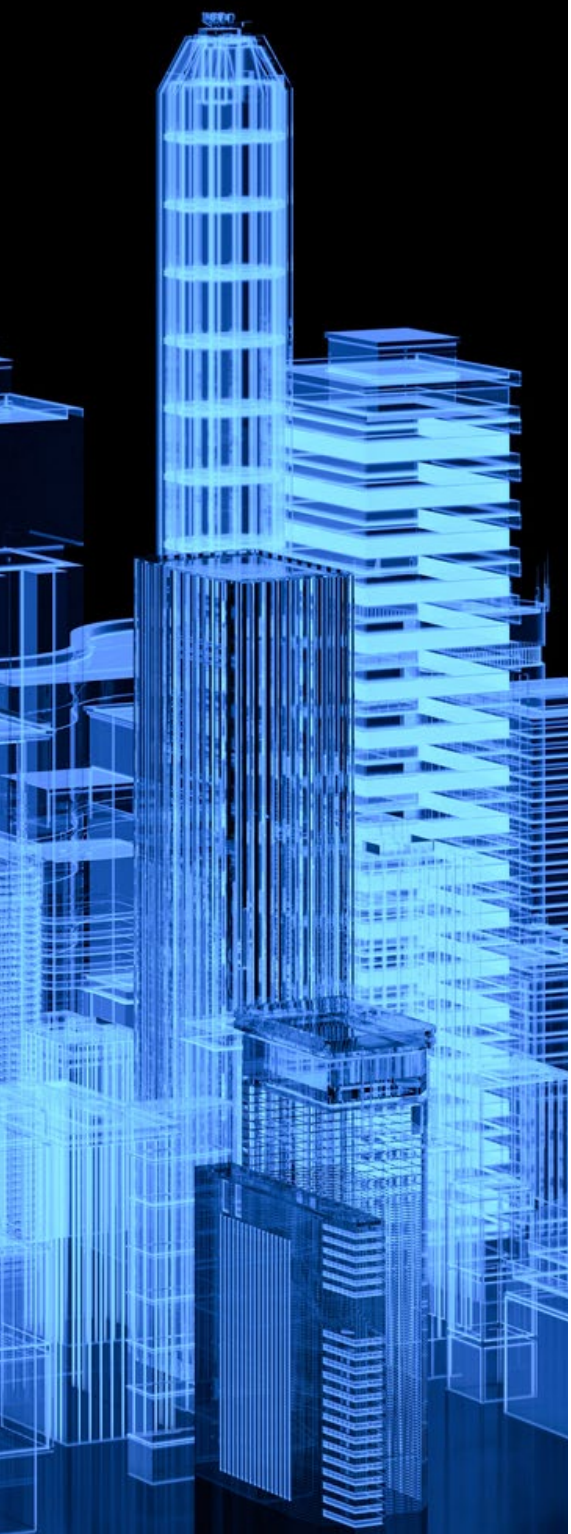
Como parte de la cobertura se encuentra:

1. Responsabilidad por la violación de datos (información) ante un ciberataque.
2. Pérdida financiera y de reputación por la falla de sistemas debido a un ataque malicioso.
3. Defensa regulatoria y laudos civiles, multas y sanciones como resultado de una violación de la seguridad, así como errores u omisiones en la protección y privacidad de la información de terceros.
4. Violaciones a la propiedad intelectual por manejo inadecuado de información y negligencia en el manejo de contenidos electrónicos.
5. Cubre los gastos de notificación, monitoreo crediticio y reducción de la utilidad por interrupción del negocio. Además, ampara los gastos para la recuperación y/o reconstrucción de datos, inclusive por el uso de profesionales externos.
6. Los daños y gastos por ciber extorsión, así como los gastos de manejo de crisis.

Un ataque cibernético puede tener ramificaciones de gran alcance para el sector de la Hospitalidad. Entender estos riesgos y de manera proactiva mitigarlos es la clave. En Lockton, entendemos las muchas presiones y desafíos a los que se enfrenta el Sector, por lo que con nuestro equipo de expertos trabajaremos con usted para crear una solución personalizada.

La seguridad de la información de sus clientes está en sus manos.
Coloque la seguridad de su negocio en las nuestras.





Maria Antonieta Castañeda
Subdirector Comercial P&C
Hospitality & Leisure
LOCKTON MÉXICO

antonieta.castaneda@lockton.com
Tel: 55 5980 4300
Cel: 55 6603 3453

Ricardo Millán
Head ProFin México
LOCKTON MÉXICO

ricardo.millan@lockton.com
Cel: 55 4386 3224

UNCOMMONLY INDEPENDENT

