Terrorism and Security Threats for Hospitality Meeting Kit – Spanish

QUÉ ESTÁ EN RIESGO

Desgraciadamente, el sector de la hostelería está en el punto de mira del terrorismo debido a su carácter abierto y a la gran afluencia de público. Hoteles, complejos turísticos y restaurantes son considerados objetivos fáciles por los terroristas, lo que significa que son más fáciles de infiltrar que los edificios fuertemente vigilados. Esta vulnerabilidad puede tener consecuencias devastadoras.

CUÁL ES EL PELIGRO

Los riesgos del terrorismo y las amenazas a la seguridad para el sector de la hostelería son importantes y diversos, y plantean retos que requieren medidas proactivas para mitigar los posibles daños.

Algunos de los principales riesgos son:

- **Atentados Terroristas:** Los atentados terroristas pueden ocurrir de forma inesperada y provocar miedo entre los viajeros, lo que se traduce en una disminución de los viajes a los lugares afectados.
- **Ciberataques:** El sector hotelero es vulnerable a las amenazas cibernéticas, incluidas las violaciones de datos que pueden comprometer la información de los huéspedes y los sistemas financieros.
- **Entrada no Autorizada:** Los hoteles se enfrentan al riesgo de que personas no autorizadas accedan a zonas restringidas, lo que compromete la seguridad y puede poner en peligro a los huéspedes y al personal.
- **Violencia y Acoso:** En los hoteles pueden producirse

incidentes de violencia, acoso o agresión, que afectan tanto a los huéspedes como a los empleados.
- **Robo:** El robo es una amenaza de seguridad común en los hoteles, que implica el robo de pertenencias personales, el robo de empleados y el robo en las zonas de aparcamiento.

COMO PROTEGERSE

He aquí una respuesta ampliada sobre las precauciones de seguridad de las empresas de hostelería frente al terrorismo y las amenazas a la seguridad:

Medidas de Seguridad Física:

- Aplique un enfoque de seguridad por niveles que combine el control de acceso, la vigilancia y la disuasión. Esto podría implicar la instalación de detectores de metales y cámaras de seguridad en las entradas, el empleo de guardias de seguridad para patrullar las zonas públicas y gestionar el acceso a las zonas sensibles, y la utilización de bolardos o barreras para restringir el acceso de vehículos a los edificios.
- Organice sesiones informativas periódicas sobre seguridad para el personal, familiarizándolo con los protocolos para identificar paquetes o comportamientos sospechosos, y facultándolo para informar de cualquier preocupación a los supervisores.
- En función de la evaluación de riesgos, considere la posibilidad de implantar un sistema de control de equipajes, especialmente para huéspedes de alto perfil o en lugares con un nivel de amenaza más elevado.
- Asegúrese de que las habitaciones de los huéspedes tengan cerrojos y mirillas que funcionen y considere la posibilidad de ofrecer a los huéspedes cajas de seguridad para los objetos de valor.

Preparación y Respuesta ante Emergencias:

- **Plan de Respuesta ante Emergencias:** Elabore un plan integral de respuesta a emergencias que describa los procedimientos

para diversas amenazas, como incendios, tiradores activos, amenazas de bomba y catástrofes naturales. Forme periódicamente al personal en el plan, garantizando la claridad de las funciones y los protocolos de comunicación.

- **Simulacros de Evacuación:** Realice simulacros de evacuación periódicamente, simulando diferentes situaciones de emergencia y asegurándose de que los huéspedes y el personal están familiarizados con las vías de evacuación y los puntos de reunión.
- **Suministros de Emergencia:** Mantenga un inventario bien abastecido de suministros de emergencia, incluidos botiquines de primeros auxilios, extintores y agua embotellada, colocados estratégicamente en toda la propiedad.

Medidas de Ciberseguridad:

- **Cifrado de Datos:** Implemente prácticas de cifrado de datos para salvaguardar la información de los huéspedes, los datos financieros y las operaciones internas del acceso no autorizado.
- **Capacitación Sobre Ciberseguridad:** Eduque al personal sobre las mejores prácticas de ciberseguridad, incluida la higiene de contraseñas, el reconocimiento de correos electrónicos de phishing y la importancia de informar sobre actividades sospechosas en línea.
- **Actualizaciones Periódicas del Sistema:** Asegúrese de que todos los sistemas informáticos y el software se actualizan regularmente con los últimos parches de seguridad para hacer frente a las vulnerabilidades.

Las medidas concretas que adopte en caso de atentado terrorista o situación de seguridad dependerán de las circunstancias exactas. Sin embargo, aquí tienes una guía general sobre qué hacer en varios escenarios:

Si hay un Tirador Activo:

- **Corra si puede escapar con seguridad.**
- **Escóndase si no es posible escapar.** Busque un lugar seguro

para esconderse, fuera de la vista del tirador. Silencie su teléfono e intente mantener la calma.
- **Luche como último recurso.** Defiéndase sólo como último recurso si su vida está en peligro inmediato.

Si hay una Amenaza de Bomba:

- No toque ni mueva el objeto sospechoso.
- Evacue la zona con calma y siga las instrucciones de las fuerzas del orden.
- Informe inmediatamente de la amenaza a un miembro del personal o al personal de seguridad.

CONCLUSIÓN

Recuerde que lo más importante es mantener la calma y tomar medidas para protegerse. En cualquier situación, dé prioridad a su seguridad y siga las indicaciones de las fuerzas del orden o del personal de seguridad del hotel.