Amenazas en el Sector Turístico

Ciberseguridad

- Conjunto de Prácticas
- Tecnológicas y Políticas
  - Sistemas Informáticos
  - Redes
  - Aplicaciones
  - Datos
    - » Contra amenazas digitales:
      - ataques maliciosos, accesos no autorizados
      - acceder, modificar o destruir información confidencial, extorsionar a usuarios o interrumpir la continuidad del negocio

Objetivo Principal

Garantizar

la Confidencialidad,
Integridad y Disponibilidad

de la información digital

CIA (Triada)

Confidentiality, Integrity, Availability

Componentes Claves

- Seguridad de Red
- Seguridad de Aplicaciones
- Seguridad de la Información
- Recuperación ante desastres y Continuidad del Negocio
- Capacidad del Usuario Final

Objetivos

- Mantener la confidencialidad, asegurando que solo usuarios autorizados accedan a información sensible.
- Garantizar la integridad evitando modificaciones no autorizadas.
- Asegurar la disponibilidad permitiendo acceso continuo a sistemas e información cuando sea necesario.

Características Claves

- La **Integridad de los datos,** Garantizar la integridad evitando modificaciones no autorizadas
- **Confidencialidad,** tener la confidencialidad asegurando que solo usuarios autorizados accedan a información sensible.
- **Disponibilidad,** Asegurar la disponibilidad permitiendo acceso continuo a sistemas e información cuando sea necesario

Detección y Respuesta rápida ante peligros

Prevención de riesgos.

Las empresas preparan a un equipo en seguridad para ser garante de estas características y lograr una confianza en los clientes, lo que ayuda a mantener su imagen.

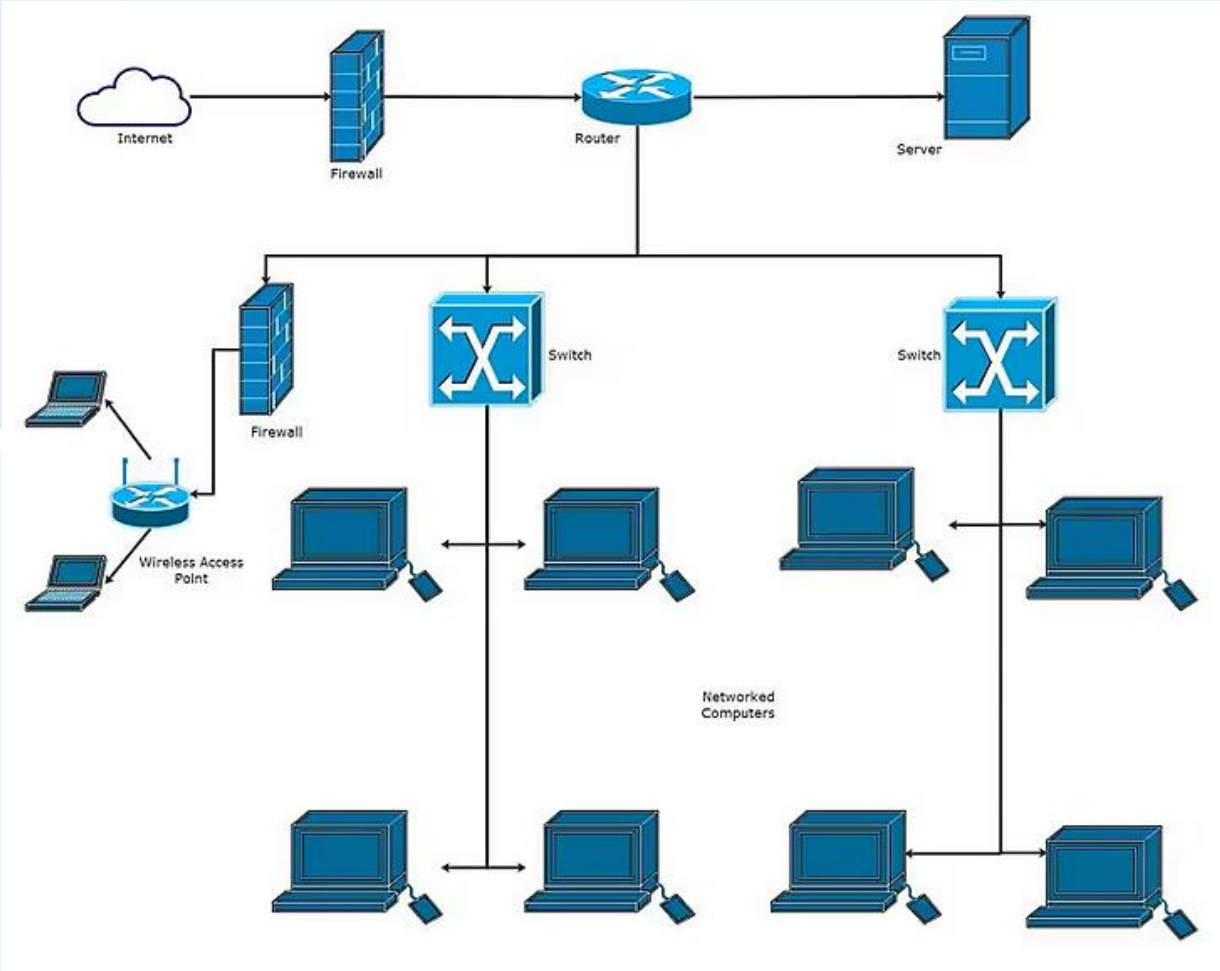
Pilares de la Ciberseguridad

- Los tres tipos principales de ciberseguridad son **la seguridad de la red, la seguridad de la nube y la seguridad física**.

- Los sistemas operativos y la arquitectura de la red conforman la seguridad de nuestra red. Puede incluir protocolos de red, cortafuegos, puntos de acceso inalámbricos, hosts y servidores.


Ciberseguridad

Esquema


Internet
Firewall
Router
Server
Firewall
Switch
Switch
Wireless Access Point
Networked Computers

Ataques más comunes

- **Malware:** software malicioso que se instala en un dispositivo sin autorización del usuario
- **Phishing:** Son técnicas que buscan engañar a la victima, ganado su confianza haciéndose pasar por una persona, empresa o servicio de confianza
- **RasonWare:** es un código malicioso que impide la utilización de los equipos o sistemas instalados
- **Cryptojacking:** Son programas tipo troyanos que se instalan en el dispositivo sin consentimiento para aprovecharse de los recursos de éste con el objetivo de minar criptomonedas

¿Qué es la seguridad turística según la OMT?

Entendemos por seguridad turística **la protección de la vida, de la salud, de la integridad física, psicológica y económica de los visitantes, prestadores de servicios y miembros de las comunidades receptoras**

(Organización Mundial del Turismo).

El sector turístico se enfrenta a grandes amenazas de ciberseguridad como:

- **Robo de información** (para venderlo en el mercado negro); ataques que provocan la disrupción del negocio (no permiten a las compañías prestar los servicios)

- **Ataques que afectan a la calidad del servicio** (degradan la experiencia del usuario). Los datos muestran que el 89% de los ciberataques tienen motivos financieros y de espionaje, lo que pone de manifiesto que cualquier información puede ser monetizable.

- El riesgo en el sector turístico se incrementa en su cadena de valor, en la que **aparecen negocios de terceros que completan la propuesta**, añadiendo nuevos riesgos sobre la seguridad de los datos de sus clientes y de la propia compañía.

- **Pérdida de confianza de los clientes**, daño a la reputación de la marca, pérdidas económicas y riesgos legales son unas de las principales **consecuencias** del ciberataque en la industria turística.

Los Ciberriesgos en el Sector Turístico

- El sector turístico está formado por diferentes tipos de empresas, que van desde alojamientos y restaurantes hasta operadores o compañías de alquiler de vehículos.

- Todos estos **negocios están cada día más conectados digitalmente**, muchos dependen de tecnologías en la nube (como plataformas de gestión de clientes o pasarelas de comercio y pago electrónico), internet de las cosas o herramientas de análisis de datos.

En función del nivel de madurez digital y de dependencia tecnológica también varía el nivel de riesgo cibernético al que tienen que hacer frente las empresas del sector turístico.

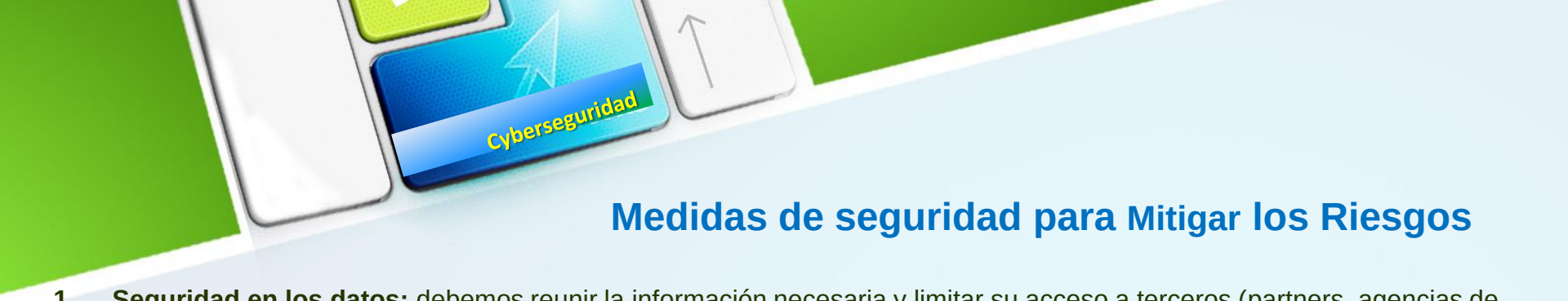
Principales Amenazas en el Sector Turístico

- **Amenazas a través de correo electrónico**
  - Fraude del CEO
  - Utilizan técnicas de Deep fake
- **Amenazas al sitio web corporativo**
  - Fuga de información confidencial
  - Denegación de servicio
  - Defacement
- **Amenazas en las redes sociales**
  - Fraudes de suplantación de identidad
- **Amenazas a través de las redes Wifi**
  - Ataques de man-in-the-middle (ciberdelincuente entre receptor y emisor para sustraer info)
  - Eavesdropping (captura trafico de red no autorizado)

Medidas de Seguridad y Buena Práctica

- **Control de acceso a la información (política de seguridad)**
- **Copias de seguridad (política de respaldo y recuperación)**
- **Gestión de contraseñas (políticas – estándares de acceso)**
- **Cifrado de datos (BD, SO, APP, antivirus)**
- **Actualizaciones (actualiz. Patches, firmware)**
- **Eliminación segura de la información**
- **Control de uso de herramientas corporativas**
- **Confidencialidad en la contratación de servicios**
- **Cumplimiento legal**. LO de delitos informáticos y Ley Prot. De Datos Personales
  - Decreto 1204 de 2001

Además de contar con la plataforma tecnológica adecuada que gestione la información, es muy importante implicar a empleados o colaboradores en la importancia de la formación y concientización en materia de ciberseguridad.



Medidas de seguridad para Mitigar los Riesgos

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

2. **Control de accesos a los datos más sensibles:** restringir el acceso de datos sensibles a los empleados y limitar el número de accesos de administrador.

3. **Monitorización y segmentación de la Red:** se aconseja monitorizar la Red 24x7 y localizar los datos más sensibles en un lugar más seguro.

4. **Securización de accesos remotos:** se recomienda limitar el acceso para clientes y empleados que acceden remotamente.

5. **Exigir medidas de seguridad a proveedores de servicios.** Por ejemplo, debemos exigir seguridad de aplicaciones desarrolladas por terceros.

6. **Reducir la exposición a los ciberriesgos** contando con las **barreras tecnológicas adecuadas** (como los antivirus, los certificados de seguridad, las pasarelas de pago seguro o los programas de gestión de contraseñas robustas)

7. **Reforzar la cultura corporativa y la capacitación** de los empleados para que estén atentos a comportamientos sospechosos y no cometan errores que puedan comprometer la seguridad de la empresa y de sus clientes.

8. **Adquirir seguros de ciberriesgos:** son una herramienta de mitigación fundamental para proteger el balance y la cuenta de resultados de las empresas del sector turístico. Al cubrir los daños propios derivados de un ciberataque: gastos de especialistas para gestionar el incidente; asesoramiento legal en caso de notificación por compromiso de datos personales, gastos de recuperación de datos, así como la pérdida del beneficio neto y los extracostes derivados de una interrupción de redes y sistemas. Adicionalmente se cubre también el perjuicio económico ocasionado al tercero como consecuencia del fallo de seguridad.

Principales Malware

1. Virus Informáticos: Son programas que se replican y pueden dañar archivos o sistemas al ser ejecutados. Requieren la interacción del usuario para propagarse.

2. Gusanos: Se propagan automáticamente a través de redes sin necesidad de archivos adjuntos, explotando vulnerabilidades en los sistemas.

3. Troyanos: Entrar en un sistema disfrazados como aplicaciones legítimas, permitiendo el acceso no autorizado o la descarga de más malware.

4. Ransomware: Cifran los datos del usuario y exigen un rescate para desbloquearlos, siendo una amenaza significativa por su capacidad para secuestrar información crítica.

5. Spyware: Monitorean las actividades del usuario sin su conocimiento, recopilando información sensible como contraseñas o números de tarjeta.

6. Adware: Muestra anuncios no deseados y puede recopilar datos sobre el comportamiento del usuario en línea.

7. Phishing (aunque técnicamente no es un tipo específico de malware): Utiliza ingeniería social para engañar a los usuarios y obtener información confidencial; puede ser un vector común para distribuir otros tipos de malware.

8. Keyloggers (o registradores de teclas): Registra cada pulsación del teclado capturando contraseñas u otra información sensible.

9. Bots/Botnets: Un conjunto coordinado de dispositivos infectados utilizados generalmente para ataques DDoS o distribución masiva de spam.

Medidas de Seguridad y Buena Práctica

- GeekPrank Ventana Hacker – El Mejor Simulador de Hacking

Un hacker de sombrero es un hacker de seguridad ética.

Hacking ético es un término destinado a implicar una categoría más amplia que solo pruebas de penetración.

Bajo el consentimiento del propietario, los hackers de sombrero blanco tienen como objetivo identificar cualquier vulnerabilidad o problema de seguridad que tenga el sistema actual.

El sombrero blanco se contrasta con el sombrero negro, un hacker malicioso; esta dicotomía definitoria proviene de las películas del Oeste, donde los vaqueros heroicos y antagónicos tradicionalmente podrían usar un sombrero blanco y uno negro, respectivamente.

Los hackers de sombrero blanco también pueden trabajar en equipos llamados "sneakers y/o hacker clubs“.

Un hackeo ético a gran escala podría incluir enviar un correo electrónico al personal para solicitar los detalles de la contraseña, hurgar en los cubos de basura de los ejecutivos, generalmente sin el conocimiento y el consentimiento de los objetivos. Solo los propietarios, directores ejecutivos y miembros de la junta directiva (partes interesadas) que solicitaron una revisión de seguridad de esta magnitud lo saben. Para tratar de replicar algunas de las técnicas destructivas que podría emplear un ataque real, los hackers éticos pueden organizar sistemas de prueba clonados, u organizar un hackeo a altas horas de la noche mientras los sistemas son menos críticos. En los casos más recientes, estos hackeos se perpetúan a largo plazo (días, si no semanas, de infiltración humana a largo plazo en una organización). Algunos ejemplos incluyen dejar unidades de llave USB/flash con software de inicio automático oculto en un área pública, como si alguien perdiera la unidad pequeña y un empleado desprevenido la encontrara y la llevara.

Paises (como China, Belgica y Reino Uniido) han legalizado el hacker de sombrero blanco.