UNIDAD 10

Ciberseguridad y ciberresiliencia en las PYMEs turísticas

DIGITOUR

Co-funded by the Erasmus+ Programme of the European Union

Título del Proyecto: Building Digitalisation Readiness in the Tourism SME sector

Acrónimo del Proyecto: DIGITOUR

Nº del Proyecto: 2021-2-IE01-KA220-VET-000048348

Unidad: Ciberseguridad y ciberresiliencia en PYMEs turísticas

Grupo Objetivo Primario: PYMEs en el sector turístico

Grupos Objetivos Secundarios: proveedores expertos en FP y educación continua, representantes turísticos y formadores en las empresas.

Duración estimada: entre 120 y 150 minutos

Objetivos: Los objetivos de esta Unidad son:

- Proporcionar una comprensión de los retos, riesgos e importancia de los sistemas de ciberseguridad para las PYMEs y profesionales del sector.
- Familiarizarte con los conceptos básicos clave y los términos técnicos relacionados con el área que te ayudarán a reforzar la ciberseguridad y la ciberresiliencia de tu empresa o actividad profesional.
- Posibilitar el futuro de la industria turística con un conjunto de habilidades desarrolladas en ciberseguridad y resiliencia.

Resultados de Aprendizaje: Al completar esta Unidad, serás capaz de:

- Describir el significado de los términos "ciberseguridad" y "ciberresiliencia"y entender cómo estos son imperativos para cualquier tipo de proveedor turístico.
- Demostrar que comprendes los conceptos básicos y esenciales de la ciberseguridad y la ciberresiliencia.
- Comprender los principales riesgos y ataques cibernéticos del sector turístico.
- Conocer algunas buenas prácticas para lograr la ciberseguridad y la ciberresiliencia en las empresas.
- Analizar los principales pilares de unos cibersistemas eficaces, seguros y resilientes y conocer las principales normas de ciberseguridad y ciberresiliencia.

Índice

Este proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación es responsabilidad exclusiva de su autor. La Comisión no se hace responsable del uso que pueda hacerse de la información aquí difundida. Reproducción autorizada, con indicación de la fuente.

Co-funded by the Erasmus+ Programme of the European Union

1. Introducción: Principios rectores y definiciones

¿Qué es la ciberseguridad?

Las definiciones de ciberseguridad varían, pero en general todas apuntan a la seguridad del ciberespacio, siendo éste el espacio dinámico y virtual que conecta diferentes sistemas informáticos.

Fuente: Morocco is not a cyber jungle, defense administration tells Amnesty

La ciberseguridad se compone de **2 términos clave**:

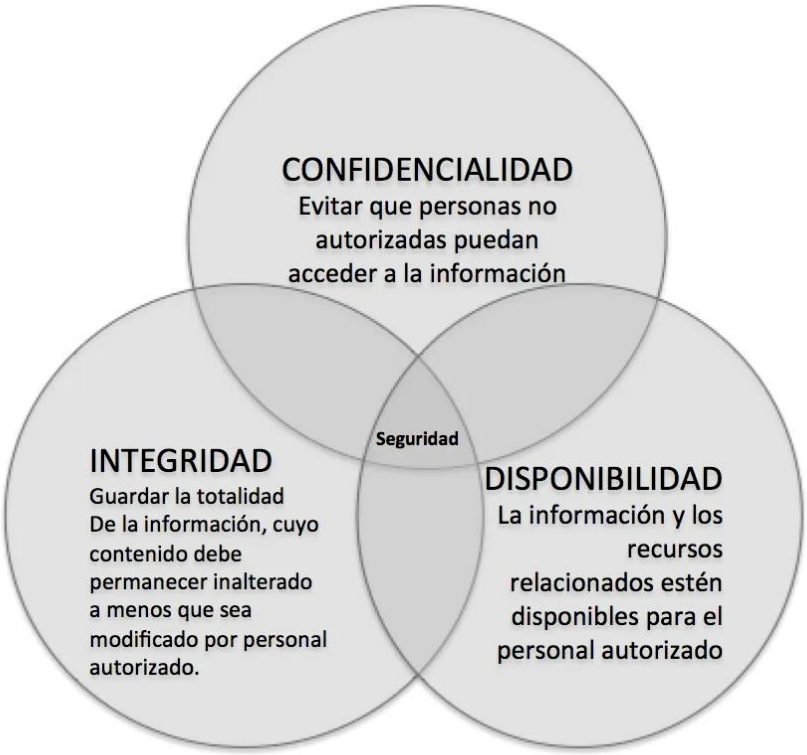
1. "Ciber" se refiere a la tecnología que contiene sistemas, redes y/o datos.
2. La parte de "seguridad" hace referencia a la protección que incluye la seguridad de los sistemas, la seguridad de las redes y la seguridad de las aplicaciones y de la información.

Por su parte, la UE define la ciberseguridad como "*las actividades necesarias para proteger las redes y los sistemas de información, a los usuarios de dichos sistemas y a otras personas afectadas por las ciberamenazas*".

Confidencialidad, integridad y disponibilidad se conocen como la tríada CIA (por sus siglas en inglés de: *Confidentiality, Integrity* y *Accessibility)*, los 3 principios fundamentales de la ciberseguridad.

- ***Confidencialidad:*** las medidas de confidencialidad impiden que la información sensible sea revelada a accesos no autorizados (por ejemplo, mediante cifrado de datos, autenticación de dos factores, etc.).

- ***Integridad:*** las medidas de integridad mantienen la coherencia, exactitud y fiabilidad de los datos a lo largo de todo su ciclo de vida, impidiendo que sean modificados por personas no autorizadas (esto se consigue, por ejemplo, mediante copias de seguridad de los datos, uso de permisos de archivos, etc.).
- ***Disponibilidad:*** las medidas de disponibilidad garantizan que la información sea accesible de forma constante y rápida para las partes autorizadas en cuestión y mantienen los sistemas de hardware y software que contienen y muestran dicha información.



Fuente: La Disponibilidad como el primero de los 3 ejes fundamentales de la Ciberseguridad Industrial

En general, la ciberseguridad se refiere a todos los aspectos de la protección de una organización, sus empleados y sus activos contra las amenazas o ataques cibernéticos.

¿Qué es la ciberresiliencia?

En el mundo empresarial, la ciberresiliencia ofrece una forma más holística de continuidad digital de la empresa. Se trata de un nuevo concepto, denominado aptitud digital.

La UE define la ciber resiliencia como *"la capacidad de proteger los datos y sistemas electrónicos de los ciberataques, así como de reanudar rápidamente las operaciones empresariales en caso de que un ataque tenga éxito".*

En el sofisticado entorno de las amenazas digitales, las tácticas tradicionales de seguridad centradas en la ciberseguridad están fracasando. Ninguna organización puede al mismo tiempo cribar alteraciones, rastrear vulnerabilidades y aplicar políticas de seguridad en varios sistemas de manera eficiente. Por ello, para gestionar estos retos contrapuestos, las organizaciones deben cambiar su postura de seguridad de una postura defensiva centrada en el malware a un enfoque más realista y resistente: un enfoque de ciberresiliencia (Symantec, 2014).

El concepto de ciberresiliencia puede concebirse como un marco con 5 pilares principales, como son:

1. **Preparar/Identificar:** comprender la seguridad de la empresa e identificar posibles posturas de riesgo para abordar las vulnerabilidades de seguridad.

2. **Proteger:** comprender el panorama de amenazas de la empresa (por ejemplo, su nivel de vulnerabilidad y tolerancia al riesgo) garantiza una infraestructura de protección.

3. **Detectar:** una vez implantadas las medidas de protección, pueden establecerse las actividades adecuadas para detectar rápidamente un ataque, evaluar los sistemas afectados y garantizar una respuesta oportuna.

4. **Responder:** esta fase es crucial para proporcionar orientación sobre qué actividades pueden ayudar a acelerar el tiempo de respuesta y contener el impacto de un ataque una vez detectado.

5. **Recuperar:** desarrollar e implantar los sistemas adecuados para la recuperación de datos en caso de ciberataque, que es un componente esencial de cualquier estrategia de seguridad resistente.

Fuente: How to build a cyber-resilient infrastructure | AMDH Services Limited *(recurso en inglés, puedes usar el traductor de tu navegador para acceder a los contenidos en español)*

¿Qué relación existe entre ciberseguridad y ciberresiliencia?

La ciberseguridad y la ciberresiliencia pueden parecer a menudo intercambiables, ya que ambas están relacionadas, en términos generales, con la seguridad online en entornos digitales; sin embargo, no son lo mismo:

- Mientras que la ciberseguridad se refiere a una organización que limita sus amenazas centrándose en disposiciones proactivas contra la creciente proliferación de ciberataques,
- La ciberresiliencia, en cambio, se refiere a una organización que limita en la medida de lo posible los daños potenciales y las pérdidas asociadas una vez que ya se ha producido un ataque, al tiempo que reanuda su actividad con normalidad.

2. Ciberseguridad y ciberresiliencia en contexto

Ciberseguridad y ciberresiliencia en el turismo

En el contexto del turismo y de los viajes, la digitalización se ha convertido en un fuerte facilitador de los negocios en el mundo digital actual.

La ciberseguridad y la ciberresiliencia son tan importantes como la innovación digital que salvaguardan:

- La innovación digital ha redefinido la experiencia turística y ha provocado una mayor susceptibilidad del turismo a los riesgos de seguridad.

- La ciberseguridad y la ciberresiliencia son herramientas que dan forma al sector y garantizan un futuro más seguro para el sector de las PYMEs del turismo y los viajes.

La tecnología desempeña ahora un papel integral en casi todos los aspectos de la experiencia de los viajes y el turismo, desde inspirar a los turistas durante la fase previa a la compra del viaje del consumidor, hasta dejar opiniones online en la fase posterior a la compra.

Esto implica a menudo transacciones en línea, información confidencial de los clientes, integración en la nube y tecnología de pago digital, lo que ha aumentado la huella digital de las empresas turísticas, exponiéndolas a ciberamenazas y ataques, algunos de los cuales pueden constituir ciberdelincuencia (Paraskevas, 2020).

Fuente: Emmanuel Fesobi, Author at Cyberverdict

Desde 2010 se han registrado varias violaciones de la ciberseguridad, incluso en las mayores cadenas hoteleras del mundo.

Uno de los casos más sonados fue el del Marriott International Hotel Group. Esta cadena hotelera fue responsable de una violación de datos en 2020 al no proteger debidamente los datos personales de sus clientes, revelando así nombres, direcciones postales, números de cuentas de fidelización y otra información sensible.

Aproximadamente 340 millones de huéspedes se vieron afectados por este ataque. 2 años antes, en 2018, Marriott recibió una alerta de una herramienta de seguridad interna sobre un intento de acceso no autorizado en su base de datos de reservas de huéspedes en Estados Unidos. Una investigación posterior realizada por expertos en ciberseguridad reveló que ya en 2014 se había producido un acceso no autorizado al sistema de reservas del hotel (Secure Stay, 2020).

Para saber más al respecto, puedes echar un vistazo al siguiente recurso: For Marriott Hotels, Lightning Does Strike Twice In New Data Breach Affecting 5.2 Million - Grit Daily News *(recurso en inglés, puedes usar el traductor de tu navegador para acceder a los contenidos en español).*

Como vemos, las repercusiones de las amenazas y/o ataques cibernéticos pueden causar un daño considerable a la reputación de la marca y a la confianza de los consumidores en la misma, lo que se traduce en importantes consecuencias financieras, legales y normativas. Así pues, los proveedores turísticos pueden sufrir tanto pérdidas financieras directas como indirectas (Paraskevas, 2020), algunas de ellas como:

- **Pérdidas financieras directas**: gastos de la empresa asociados a los servicios de recuperación de IT, así como honorarios legales y servicios de relaciones públicas.
- **Pérdidas financieras indirectas**: costes de contratación de personal informático técnico adicional, formación del personal en ciberseguridad y ciberresiliencia, actualización de las infraestructuras de ciberseguridad, etc.

- **Costes de reputación**: si se produce una violación de datos, también hay que tener en cuenta los costes de reputación. Los costes de reputación pueden ser asombrosos y provocar una disminución de la confianza de los consumidores y, consecuentemente, de las ventas o reservas. Los proveedores turísticos deben reconocer su responsabilidad de mantener los datos y la información seguros para evitar impactos negativos sustanciales en su negocio.

Por lo tanto, es crucial que las empresas, especialmente las PYMEs, y profesionales del sector turístico comprendan la importancia de implementar la ciberseguridad y la ciberresiliencia como prioridades para su negocio, en lugar de como una ocurrencia a destiempo.

Desarrollos posteriores al Covid-19

Tras una pandemia mundial que obligó a la industria turística a virar mayoritariamente al entorno online, el sector de los viajes y el turismo tuvo que redefinir sus productos, servicios y experiencias de consumo para hacer frente a la nueva realidad.

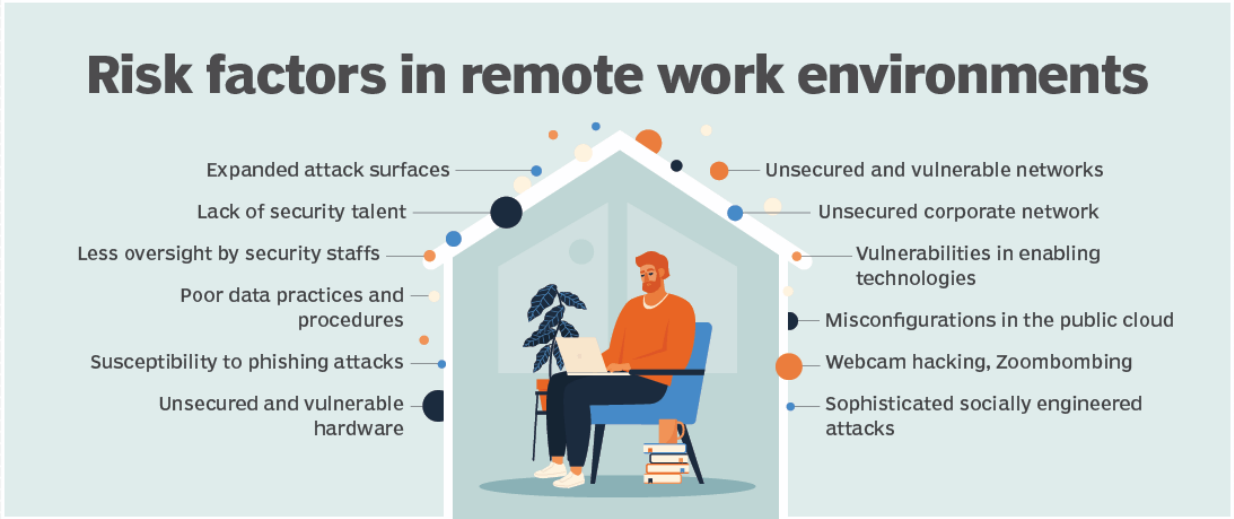
En la era posterior a Covid-19, el número de ciberamenazas nunca había sido tan elevado. En este sentido, el Consejo Mundial de Viajes y Turismo (WTTC, 2022) informa de que el crecimiento acelerado de las operaciones digitales ha dejado al sector más vulnerable y expuesto a los riesgos cibernéticos.

Esto ha animado a las empresas a revisar su postura de seguridad para construir una empresa más resistente a los ciberataques, y a implementar soluciones de ciberseguridad y ciberresiliencia en la medida de lo posible.

Fuente: Understanding Digital Forensics: Process, Techniques, and Tools (*recurso en inglés, puedes usar el traductor de tu navegador para acceder a los contenidos en español).*

Los actores de las ciberamenazas son ágiles y vieron en Covid-19 una oportunidad para explotar las vulnerabilidades de los proveedores turísticos que intentaban facilitar los viajes y, al mismo tiempo, proteger la salud pública. Las continuas e incoherentes restricciones acontecidas durante estos meses crearon un amplio margen para los ciberataques.

Por ejemplo, la adopción del trabajo a distancia, que ha dado lugar a una mayor dependencia de los dispositivos personales y móviles, ha hecho recaer cada vez más en los empleados la responsabilidad de la ciberseguridad de la empresa.



Fuente: Securing remote access grows crucial for DevSecOps | TechTarget (*recurso en inglés, puedes usar el traductor de tu navegador para acceder a los contenidos en español)*

Aunque los ecosistemas cibernéticos *in situ* de las grandes empresas suelen ser seguros, hasta ahora esta seguridad no se había extendido a los hogares de los empleados. Como resultado, los atacantes que accedían a las redes Wi-Fi domésticas o públicas podían vulnerar fácilmente los sistemas de la empresa, lo que pone de relieve la necesidad de un enfoque más integral de la ciberseguridad, que haga hincapié en la resiliencia cibernética a todos los niveles.

Aunque las organizaciones no pueden garantizar la seguridad de las redes Wi-Fi domésticas o públicas, en este caso la formación del personal sí puede ayudar a proteger a los empleados contra las amenazas cuando utilizan dispositivos IoT (internet de las cosas, por sus siglas en inglés de *Internet of Things*).

Las amenazas cibernéticas resultantes de COVID-19 no deben tratarse como independientes del riesgo organizativo, incluidos los riesgos cibernéticos asociados a los modelos de trabajo híbridos.

Por ello, para garantizar la resistencia cibernética, las organizaciones deben ampliar sus esfuerzos de vigilancia de amenazas para abarcar posibles puntos de entrada de ataques a través de sistemas Wi-Fi domésticos y públicos, (Consejo Mundial de Viajes y Turismo y Microsoft, 2022).

3. La ciber vulnerabilidad de las PYMEs turísticas

¿Cuál es la vulnerabilidad de las PYMEs turísticas?

El WTTC informa de que más de 7 de cada 10 (72%) PYMEs del Reino Unido, EE.UU. y Europa han sido víctimas de al menos 1 ciberataque, (Consejo Mundial de Viajes y Turismo y Microsoft, 2022).

En el sector de los viajes y el turismo, compuesto en su mayoría por PYMEs como agencias y operadores turísticos, el porcentaje es aún mayor, ya que las PYMEs representan alrededor del 80% de todas las empresas.

"¿Sabías que cada 39 segundos se produce un ciberataque y cada segundo se roban 291 registros de datos?".

Fuente: Deception Technology - Mislead about true intentions or capabilities (*recurso en inglés, puedes usar el traductor de tu navegador para acceder a los contenidos en español)*

En los últimos años, las PYMEs turísticas se han convertido en un objetivo atractivo para los ciberdelincuentes, puesto que:

- El alto grado de madurez de la digitalización convierte a las PYMEs turísticas en un sector muy vulnerable en términos de ciberseguridad y ciberresiliencia, especialmente debido a las deficientes defensas de sus sistemas informáticos y puntos de venta (Fragniere & Yagci, 2021). Según Hussain (2023), los piratas informáticos se han dado cuenta de que las PYMEs son objetivos más fáciles en comparación con las grandes empresas con una ciberseguridad inadecuada, ya sea por falta de personal cualificado y capacitado (es decir, error humano) o por presupuestos insuficientes.

- Las PYMEs turísticas son especialmente vulnerables a las ciberamenazas debido a los datos y análisis altamente sensibles que almacenan en el ciberespacio, convirtiéndolos en información valiosa para los ciberdelincuentes que intentan acceder a dichos datos y violarlos, lo que conduce al robo de identidad y financiero, amenaza la gobernanza de datos y la protección de la privacidad de clientes y empleados (direcciones de correo electrónico de los clientes, números de pasaporte, datos de tarjetas de crédito, etc.).

- El sector de las PYMEs turísticas es especialmente susceptible a las ciberamenazas, ya que su naturaleza es fragmentada, y toda la cadena de suministro (en la que intervienen numerosos agentes y proveedores de servicios terceros) es un área potencial de entrada para los actores de las amenazas. Es necesario adoptar medidas proactivas de ciberseguridad para

garantizar la resistencia cibernética y mantener la eficacia de las operaciones empresariales.

La Agencia de Ciberseguridad de la Unión Europea (ENISA) descubrió que el 90% de las PYMEs declararon que los problemas de ciberseguridad tendrían graves repercusiones negativas en su negocio en el plazo de una semana desde que se produjeran, y el 57% afirmó que lo más probable es que quebraran o quebraran.

https://www.enisa.europa.eu/

¿Cómo deben responder las PYMEs en caso de violación de datos?

En caso de violación de datos, se aconseja a las PYMEs que notifique dicha violación de inmediato a las autoridades competentes. Si la violación supone un riesgo para el interesado, es necesario notificarlo a la autoridad de control.

Estas son 5 medidas concretas que puede adoptar una PYME tras una violación de datos.

1. Identificar el origen y el alcance de la violación.
2. Alertar a su grupo de trabajo y solucionar la violación lo antes posible.
3. Probar la solución de seguridad.
4. Informar a las autoridades y a todos los clientes afectados.
5. Prepararse para la limpieza posterior a la violación y el control de daños.

4. Ciberamenazas en las PYMEs turísticas

¿Qué son las ciberamenazas?

Es posible definir una ciberamenaza como "*cualquier circunstancia o evento con el potencial de afectar negativamente a las operaciones comerciales, los activos, los empleados y/u otras organizaciones, o a una nación a través de un sistema mediante el acceso no autorizado, la destrucción, la divulgación, la modificación de la información y/o la denegación de servicio*".

Existen 3 tipos principales de ciberamenazas:

1. La ciberdelincuencia incluye actores individuales o grupos que atacan los sistemas para obtener beneficios económicos o causar trastornos.

2. El ciberataque a menudo implica la recopilación de información por motivos políticos.
3. El ciberterrorismo pretende socavar los sistemas electrónicos para causar pánico o miedo.

¿Cuáles son los principales tipos de ciberamenazas en las PYMEs turísticas?

Como ya hemos visto, cuando se trata de intentos de ciberamenazas, las PYMEs del sector de los viajes y el turismo son uno de los sectores más afectados a escala mundial. Un Informe de Perspectivas Hoteleras de PwC de 2018 a 2022 afirmó que durante este período la industria hotelera tuvo el máximo número de violaciones de ciber datos después del sector minorista.

En este escenario, los ciberataques en el sector de los viajes se dirigen principalmente contra las tarjetas de crédito, la información personal identificable, los programas de recompensas de la hostelería e Internet de acceso público, (Walson, 2022).

Según el WTTC, las amenazas de phishing, malware y ransomware se mantienen constantes, con el ransomware representando el 23% de los ciberataques en 2021, y el phishing utilizado en el 33% de los ciberataques. Los ciberdelincuentes acceden en gran medida a los entornos cibernéticos a través del phishing, el robo de credenciales o el control remoto del escritorio, (Consejo Mundial de Viajes y Turismo y Microsoft, 2022).

Fuente: Top Cybersecurity Threats and Proactive Measures to Protect Personal and Business Data (*recurso en inglés, puedes usar el traductor de tu navegador para acceder a los contenidos en español)*

Los métodos más comunes utilizados por los actores maliciosos cuando intentan amenazar la ciberseguridad y la ciberresiliencia de una empresa turística son:

- **Malware:** es una de las ciberamenazas más comunes que se propaga a través de un archivo adjunto de correo electrónico no solicitado o una descarga de aspecto legítimo. El ataque de malware compromete los sistemas y datos sensibles de una organización infectándolos con software malicioso como virus, gusanos, troyanos y otros programas espía, (Paraskevas, 2020).

- **Phishing:** siempre ha sido el tipo más común de ciberataque y suele producirse a través del correo electrónico o SMS. Tiene lugar cuando los ciberdelincuentes envían correos electrónicos a las víctimas que parecen proceder de una empresa legítima (por ejemplo, un banco) y solicitan información sensible (por ejemplo, datos de cuentas bancarias, contraseñas).

- **Ataques a puntos de venta (TPV)**: también son muy comunes en el sector de los viajes y el turismo y proporcionan a los autores de las amenazas datos valiosos, incluida información sobre tarjetas de crédito, como números de tarjeta y números de identificación personal (PIN).

- ***Man-in-the-middle***: este tipo de ciberataque se produce en una red WiFi insegura en la que un actor de amenazas podría interceptar los datos que se transmiten desde el dispositivo de la víctima y la red.

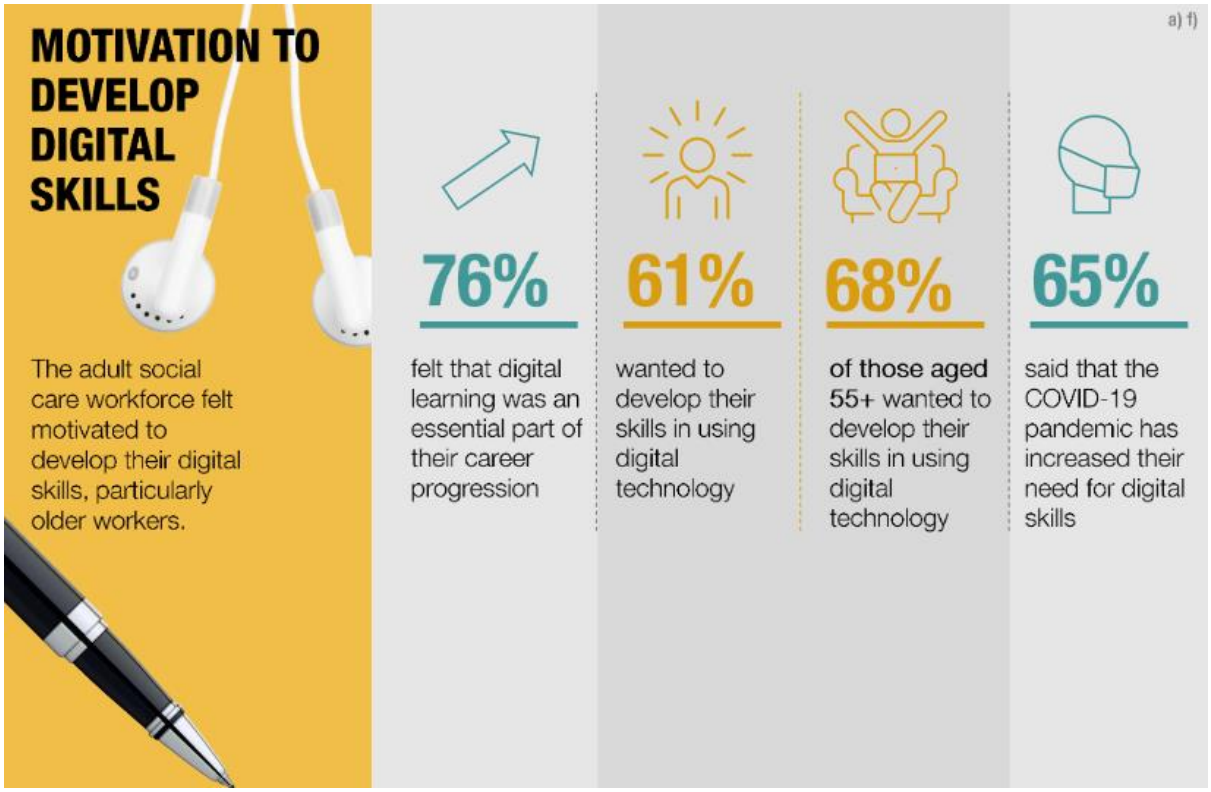
- **Ransomware**: el objetivo de esta amenaza no es robar datos, sino denegar a su propietario el acceso a ellos y hacer que el objetivo pague directamente al atacante. El ransomware está programado para identificar los datos más sensibles o valiosos de la empresa.

- **Ataques de botnet**: uso de grandes redes, a menudo compuestas por numerosos ordenadores, smartphones o dispositivos inteligentes (también conocidos como "ejércitos zombis") para llevar a cabo actividades maliciosas como intentos de inicio de sesión, ataques de spam o el secuestro de redes, dispositivos de red, sitios web o el entorno informático de una organización.

- **Ataques a terceros proveedores de servicios**: los actores de las amenazas también atacan a los miembros del "DexteR" de la organización (socios digitales y terceros proveedores de servicios), a menudo considerados los eslabones más débiles de la red y que representan atractivos puntos de agregación de datos sensibles de la empresa, (IBM 2018 citado en Paraskevas, 2020).

5. Buenas prácticas cibernéticas para las PYMEs turísticas

Un elemento crucial de la ciberseguridad y la ciberresiliencia es la educación del personal de una empresa (o el propio) y su formación en competencias digitales. Los empleados que reciben una formación adecuada sobre cómo evitar ser víctimas de ciberataques y saben qué denunciar pueden mejorar los sistemas de seguridad de una PYME turística y reducir el riesgo de ciberamenazas, como el acceso no autorizado a los cibersistemas de la empresa.



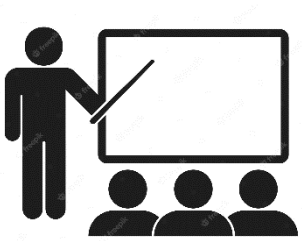
Fuente: Digital Skills & Training (*recurso en inglés, puedes usar el traductor de tu navegador para acceder a los contenidos en español)*

El WTTC identifica 7 buenas prácticas que pueden adoptarse en las pequeñas y medianas empresas para mejorar aún más la ciberresiliencia en sus operaciones:

1. Integrar la gestión del riesgo cibernético en la gestión del riesgo organizativo

Los ciberriesgos deben priorizarse y gestionarse junto con otros riesgos empresariales y operativos. Las empresas deben revisar y actualizar periódicamente sus procesos de gestión de riesgos y asignar un presupuesto acorde con el nivel de riesgo y las medidas de mitigación necesarias. Se necesitan empleados (o autónomos/as) cualificados para crear e informar sobre las políticas de ciberriesgos, aplicar las mejores prácticas y gestionar los riesgos de forma proactiva y continua.

2. Educar y formar a todo el personal



La formación es crucial para introducir nuevo personal y educar al personal actual para garantizar el uso eficaz de los sistemas y procesos digitales y la seguridad. Aunque no todos los empleados requieren el mismo nivel de formación, es importante que el personal (si lo hubiere) tenga una comprensión fundamental de los principios de ciberseguridad. Esto reduce la probabilidad de que se produzcan ciberataques por parte de personas con información privilegiada.

3. Ampliar la protección contra riesgos más allá del lugar de trabajo físico

Con el paso al trabajo remoto e híbrido, los controles cibernéticos deben aplicarse de forma más amplia. Es crucial considerar cómo los modelos de trabajo híbridos podrían afectar a la seguridad y aumentar las vulnerabilidades, incluida la seguridad Wi-Fi doméstica, la ciber higiene de los empleados en sus propios dispositivos, etc.

4. Aplicar un enfoque de confianza cero a la ciberseguridad

El enfoque de confianza cero se aleja de los métodos anteriores que se basaban en niveles más altos de confianza dentro de la organización. Así pues, este marco de actuación se basa en la verificación explícita de las solicitudes de acceso, en el acceso con menos privilegios y en la suposición de una violación o compromiso. Esto permite una mayor flexibilidad en el acceso al tiempo que limita la exposición a los sistemas centrales.

Fuente: Apply Zero Trust information security framework to ICS/OT environment

Para saber más sobre este enfoque de Confianza Cero, te recomendamos echar un vistazo a los siguientes materiales:

- ¿Qué es el modelo Zero Trust en ciberseguridad?

- ¿Qué es Zero Trust? | IBM
- ¿Qué es la confianza cero?

5. Utilizar evaluaciones continuas de las amenazas

Esto incluye mejorar la resistencia frente a las ciberamenazas estableciendo relaciones con expertos en la materia, utilizando análisis para perfeccionar las medidas de protección, realizando pruebas de penetración para identificar vulnerabilidades, segmentando los sistemas para limitar el impacto de las brechas y priorizando la protección de los sistemas.

6. Ser transparente

Es fundamental comunicar las medidas de seguridad aplicadas y los motivos de la recopilación de datos, su uso y los periodos de almacenamiento. Las PYMEs turísticas deben recopilar sólo la menor cantidad de datos personales e información de pago necesaria y ofrecer los mayores niveles de protección para fomentar la confianza de sus clientes y grupos de interés. Debe destacarse el cumplimiento de la legislación y las normas (por ejemplo, GDPR). Si se produce una violación, se debe notificar inmediatamente a las partes afectadas y a los organismos reguladores, y se deben tomar medidas para mitigar el impacto de la violación.

7. Implantar una norma organizativa

Los responsables de las empresas deben cumplir la legislación de las regiones en las que operan sus organizaciones. La misión de la UE de fomentar un enfoque normalizado de la ciberseguridad y la resiliencia y la protección de datos ha llevado al desarrollo de:

- La Ley de Ciber Resiliencia de la UE pretende establecer normas comunes de ciberseguridad para los productos digitales y los servicios asociados que se comercializan en el mercado de la UE.
- La Ley de Ciberseguridad de la UE refuerza la ENISA y establece un marco de certificación de ciberseguridad para productos y servicios.
- La evolución del panorama cibernético hace necesaria una legislación cibernética específica para mejorar la protección civil; aquí es donde entra en juego el Reglamento General de Protección de Datos (GDPR) de la UE. La prioridad actual de ENISA es fomentar las medidas de protección de datos

para mostrar cómo las tecnologías de ciberseguridad pueden apoyar el cumplimiento de los principios de protección de datos del GDPR (véanse los pasos relativos a la respuesta a la violación de datos en la sección 10.3).

- Como parte del Año Europeo de las Capacidades 2023, la Comisión adoptó una Comunicación sobre una Academia de Capacidades de Ciberseguridad el 18 de abril de 2023.

Estas normativas e iniciativas políticas deben ser tenidas en cuenta por las PYMEs turísticas a la hora de desarrollar e implantar una norma de organización, que también debería contar con la información de expertos en ciberseguridad, privacidad y legislación.

La ENISA ha elaborado una guía de ciberseguridad para PYMEs que destaca 12 pasos en los que las PYMEs pueden asegurar sus negocios. Estos pasos son los siguientes:

1. Desarrollar una buena cultura de ciberseguridad;
2. Proporcionar la formación adecuada;
3. Garantizar una gestión eficaz de terceros;
4. Desarrollar un plan de respuesta a incidentes;
5. Asegurar el acceso a los sistemas;
6. Asegurar los dispositivos;
7. Asegurar la red;
8. Mejorar la seguridad física;
9. Asegurar las copias de seguridad;
10. Utilizar la nube;
11. Proteger los sitios en línea;
12. Buscar y compartir información.

Fuente: ENISA introduces the European Cybersecurity Skills Framework - ECSO(*recurso en inglés, puedes usar el traductor de tu navegador para acceder a los contenidos en español)*

6. Conclusión

En esta Unidad se han estudiado las formas en que la ciberseguridad y la ciberresiliencia desempeñan un papel clave en las operaciones de las empresas turísticas, los problemas y riesgos que plantean los ciberataques y las buenas prácticas que las pequeñas y medianas empresas pueden implementar para mejorar la gestión de sus operaciones en línea.

Las competencias digitales pueden servir como herramienta para que el sector turístico comprenda mejor cómo la ciberseguridad y la ciberresiliencia están configurando el sector y planifique un futuro más seguro.

Adoptar la seguridad y la resiliencia como algo normal en la vida cibernética de las empresas redunda en el interés común y para ello la formación (propia o de equipos internos) es clave para la correcta adopción de prácticas de ciberresiliencia.

7. Recursos Adicionales

Lecturas Adicionales

¿En qué consiste la ciberresiliencia y cuál es su importancia? | Conexión ESAN
Ciberresiliencia: Todo lo que necesitas saber | OBS Business School.
Ciberresiliencia La Clave Para Sobreponerse Los Incidentes | INCIBE-CERT
https://www.hosteltur.com/148240_primera-guia-de-ciberseguridad-para-el-sector-del-turismo-y-ocio.html
El estado de la ciberseguridad en España
Que una impresora vulnerable no sea tu perdición: Europa anuncia el nuevo reglamento de Ciberresiliencia para exigir dispositivos IoT más seguros
Consejos de Ciberseguridad para Pymes ofrecidos por DOLBUCK - Cámara de Comercio de Sevilla
https://link.springer.com/chapter/10.1007/978-3-319-16486-1_31
https://www.ttgmedia.com/news/news/smes-at-greatest-risk-of-cyber-attacks-says-wttc-33908

https://digitalcommons.usf.edu/m3publishing/vol17/iss9781732127593/7/

https://link.springer.com/referenceworkentry/10.1007/978-3-030-05324-6_100-1

https://securestay.medium.com/the-history-of-hotels-cyber-attacks-4b6a09c8bf30

https://www.ten-inc.com/presentations/Symantec-The-Cyber-Resilience-Blueprint.pdf

https://wttc.org/Portals/0/Documents/Reports/2022/WTTC_x_Microsoft-Codes_To_Resilience.pdf

https://idpc.org.mt/report-a-breach/

https://www.whoa.com/5-steps-to-take-after-a-small-business-data-breach/

Sitios web

Curso de Introducción a la Ciberseguridad en las PYMEs Gaditanas (Presencia Virtual Online - Cádiz) | EOI

Taller de Ciberseguridad para Pymes | Fundación INCYDE

https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

https://thingscouplesdo.com/what-is-cia-triad-and-how-does-it-work/

https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity
https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes/@@download/fullReport
https://www.enisa.europa.eu/topics/cybersecurity-policy/data-protection
https://www.eurotechconseil.com/en/blog/difference-between-cyber-security-and-cyber-resilience/
https://www.goallsecure.com/cyber-security-in-travel/
https://www.i-scoop.eu/cybersecurity/cyber-resilience/
https://mbb.org.mt/wp-content/uploads/2022/12/CRA-Brief-.pdf
https://www.omnicybersecurity.com/cyber-attacks-travel-tourism-industry/
https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA
https://www.wcrcentre.co.uk/post/why-should-cyber-security-matter-to-an-sme-in-the-tourism-and-hospitality-industry

Vídeos

https://youtu.be/wgK6Evn3QUw

La ciberseguridad en las PYMES | Riesgos y beneficios de la digitalización para las empresas

Ciberseguridad en la pyme: ¿Por dónde empiezo?

Datos sectoriales ciberseguridad 2022 | #RSAC

Introduction To Cyber Security | Cyber Security Training For Beginners | CyberSecurity | Simplilearn

What You Should Learn Before "Cybersecurity" - 2023

Cyber Security In 7 Minutes | What Is Cyber Security: How It Works? | Cyber Security | Simplilearn

Tenerife, destino turístico con plan de ciberseguridad