UNIVERSITAT POLITÈCNICA DE VALÈNCIA

ADE
FACULTAD DE ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS. UPV

TÍTULO DEL TRABAJO:

"Propuesta de un modelo de valoración para la viabilidad de la seguridad informática en una PYME"

Nombre del estudiante: **JUAN JOSÉ VIDAL DOMÉNECH**

GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS
Curso Académico 2019-2020

Tutorizado por:
José Miguel Albarracín Guillem
Ignacio Gil Pechuán

"Una empresa puede gastar cientos de miles de dólares en firewalls, sistemas de detección de intrusos y el cifrado y otras tecnologías de seguridad, pero si un atacante puede llamar a una persona de confianza dentro de la empresa, y esa persona cumple, y si el atacante entra, entonces todo lo que el dinero gastado en la tecnología es esencialmente desperdiciada"

Kevin Mitnick

ÍNDICE DE CONTENIDO

ÍNDICE DE GRÁFICOS Y/O TABLAS

1.- INTRODUCCIÓN

Ante la situación de vivir en un mundo cada vez más globalizado surgen eventos positivos y negativos, en este trabajo se van a tratar las dos caras de la misma moneda con el turismo, que siempre y cuando sea responsable y sostenible permite el acercamiento entre culturas, la comprensión y la abolición de prejuicios establecidos y los nuevos horizontes abiertos en el crimen fruto de las nuevas tecnologías de información y comunicación surgidas en esta era digital.

Primeramente, se procederá a conceptuar el término pyme y estudiar los requisitos que una empresa debe cumplir para poder ser catalogada como tal. Para seguir con el tono global que rodea al trabajo, se han incluido también los requisitos de distintos países del mundo intentando dar una visión más amplia del término al lector y evitar posibles efectos de pensamiento de grupo. También se ha decidido informar sobre la informatización en las pymes españolas de modo introductorio a la parte tecnológica del trabajo.

En segundo lugar se trabajará un introducción al sector turístico, en primer lugar se tratará de forma somera tanto tanto a nivel global como europeo para posteriormente centrarse en España y más concretamente el sector hotelero definiendo los requerimientos de clasificación de los hoteles y formulando un propuesta de Pyme hotelera para el posterior análisis de su seguridad.

A continuación se nombrarán los principales servicios tecnológicos ofrecidos por el sector hotelero español de la forma más organizada posible e incluyendo las nuevas vanguardias con las que se procurará que a pesar de su bajo nivel de implementación actual alarguen en medida de lo posible la vida útil de este trabajo que que quedará obsoleto con la aparición de nuevas tecnologías.

El cuarto punto a tratar será la identificación de riesgos informáticos de los hoteles especialmente relacionados con los servicios tecnológicos antes enumerados y una introducción a la normativa ISO 27001 que trata de minimizar dichos riesgos. Antes haciendo una revisión de los principales ataques de ciberdelincuentes que sufren las empresas del sector y casos reales que muestran sus consecuencias.

Finalmente y siendo la parte más relacionada con un caso práctico del trabajo se llevará a cabo una PROPUESTA DE SEGURIDAD PARA UNA PYME HOTELERA SEGÚN LA ISO 27001 basada en la propuesta antes creada y complementada con nuevos datos. Sobre esta propuesta se llevará a cabo un análisis de riesgos y finalmente utilizando los controles de la ISO 27001 se darán unas directrices aproximadas del comportamiento que debería tener una empresa como la propuesta para cumplir con la norma.

A continuación especificamos los objetivos prioritarios del trabajo:
Como objetivo principal, nos proponemos:

- Definir una propuesta de seguridad basada en la ISO 27001 para una PYME hotelera

También nos proponemos una serie de objetivos secundarios, que enumeramos a continuación:

- Analizar los conceptos básicos a nivel internacional relacionado con las pymes
- Estudiar la estructura de las PYMES españolas y su nivel de informatización, incidiendo en el sector hotelero.
- Describir el sector turístico dentro de la economía global y su importancia en la economía española
- Conocer la importancia de los hoteles en el sector turístico y su categorización.
- Establecer un acercamiento a los servicios tecnológicos ofrecidos en el sector hotelero español.
- Conocer los ataques informáticos más frecuentes e ilustrar su alcance a través de ejemplos reales.
- Realizar una identificación de riesgos y conocer las ISO 27001/2

Y por último, incluir la relación de asignaturas de la titulación y de la otra titulación cursada.
Para realizar el trabajo se han utilizado en mayor o menor medida contenidos impartidos en diversas asignaturas cursadas durante el grado.
En orden cronológico y por curso, indicamos las asignaturas con mayor influencia en el desarrollo del trabajo:

- 1 curso: Introducción a la administración de empresas
- 2 curso: Economía española y Economía mundial
- 4 curso : Introducción a la auditoría
- 5 curso: Gestión de servicios de SI/TI y Sistema integrados de información en las organizaciones

Nótese que dada la naturaleza tecnológica del trabajo se ha decidido también incluir algunas asignaturas de la titulación de Ingeniería informática.

2. IDEAS BÁSICAS SOBRES LAS PYMES

La pequeña y mediana empresa (PYME) ha sido, en los últimos años, el centro de atención de numerosos trabajos y estudios debido fundamentalmente a su gran capacidad de generación de empleo, así como al papel primordial que juegan como generadoras de riqueza. Esto ha permitido un mayor conocimiento sobre sus características y sus relaciones con el entorno económico.
No obstante, las PYME siguen necesitadas de fundamentos operativos que, de forma continua, pongan de manifiesto su problemática y sus estrategias al objeto de facilitar la toma de decisiones, tanto desde un punto de vista de política interna de la empresa para su gestión, que es la que nos interesa fundamentalmente en este trabajo, pero también de política regional o estatal, para determinar y fijar programas de actuación acertados.

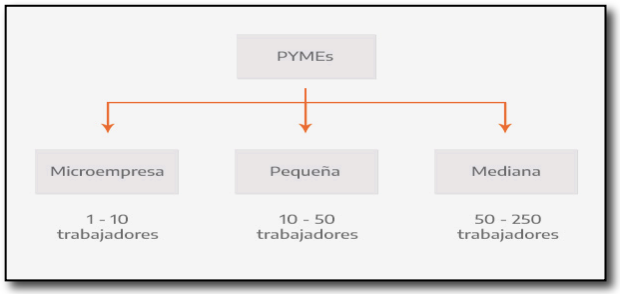
2.1. Concepto de PYME

* Según la RAE, PYME es el acrónimo de pequeña y mediana empresa.
Se caracteriza por ser una empresa compuesta por un número reducido de trabajadores, y con un moderado volumen de facturación. Esta es la esencia de lo que habitualmente entiende cualquier persona no especializada.

* Según enciclopediaeconomica.com, las PYMES son pequeñas y medianas empresas, las cuales poseen un límite en cuanto su cantidad de puestos de trabajo y capital.
Una empresa es considerada PYME cuando posee entre 1 y 250 empleados, aunque esto puede variar también según su nivel de facturación.
Las PYMES se caracterizan por promover la innovación trabajando con la lógica, los intereses y la cultura. Se encuentran directamente relacionadas con el mercado o el comercio pero casi nunca con el mercado industrial, debido entre otras cosas a las grandes inversiones que este demanda.
Las principales características de las PYMES son las siguientes:

- Son empresas heterogéneas y diversas.
- Poseen entre 1 y 250 trabajadores.
- Son independientes y cumplen un papel fundamental en la economía de un país.
- Sus costos de inversión no suelen ser elevados.
- Pueden convivir y producir en un mismo sector, con diferentes cantidades de trabajadores o producción.
- No suelen actuar en mercados internacionales.

Teniendo en cuenta que los balances o volúmenes de negocios varían de acuerdo con cada país, las PYMES pueden clasificarse de la siguiente manera:



Se entiende por :
1.- Microempresa: Aquellas empresas que poseen hasta 10 trabajadores y un balance de ingresos relativamente bajo.
2.- Pequeña empresa: Tipo de empresa que dispone de entre 10 y 50 trabajadores y posee balances de negocios medios.
3.- Mediana empresa: Empresa que posee entre 50 y 250 trabajadores, y un balance de negocios mayor al anterior.

Las PYMES son una parte importante dentro de la economía de un país debido a sus contribuciones y repartición de bienes y servicios. Se puede considerar que son las principales encargadas de generar empleos en un país pero también fomentan el mercado, la competencia y la producción nacional.

* La Unión Europea establece su definición de PYME en el Anexo I del Reglamento (UE) 651/2014 de la Comisión. Y considera PYMES las empresas que ocupan a menos de 250 personas y cuyo volumen de negocios anual no excede de 50 millones de euros, o bien cuyo balance general anual no excede de 43 millones de euros. Por tanto, para poder ser considerado PYME es necesario primero ser considerado empresa. Esta definición se aplica a todos los programas de ayudas públicas desarrollados y gestionados por la Comisión Europea.
* Pero en otros contextos se utilizan otras definiciones. Por ejemplo:
- En el ámbito contable, el Plan General de Contabilidad de PYMES puede ser aplicado voluntariamente por las empresas que no superen determinados umbrales (distintos a los de la UE).
- En el ámbito fiscal, la Ley del Impuesto de Sociedades establece incentivos fiscales para "entidades de reducida dimensión", considerando únicamente el volumen de facturación.

* Y Por último, añadir el nombre en inglés de “pyme” ya que en muchos estudios y trabajos se utiliza ese término. Se conoce como SME (small or medium sized business).

2.1.1. A nivel europeo

Para acercarnos al objeto del presente trabajo, procedemos a enumerar los distintos métodos para catalogar a una empresa como PYME, término que engloba microempresas, pequeñas y medianas (ya especificadas en algunos de los conceptos de PYME). En este punto describiremos las distintas clasificaciones de Europa, ya que son a las que se acoge España.
Y siguiendo las aportaciones del artículo: “Las MIPyMEs en el mundo: elementos para una redefinición” de la revista “Debate económico” vamos a realizar un recorrido de las distintas clasificaciones de las empresas, tanto a nivel europeo como mundial.
En primer lugar, nos centramos en la visión de la Organización para la Cooperación y el Desarrollo Económico **(OCDE)**, su sistema de clasificación se basa meramente en la cantidad de trabajadores tal y como se puede ver en la tabla adjunta.

Tabla 1. Clasificación de empresas de acuerdo con la OCDE

Clasificación	Micro	Pequeñas	Medianas	Grandes
N° de Trabajadores	1 a 19	20 a 99	100 a 499	500 a +

Fuente: Elaboración con base a Garza Cantaño Ricardo. (2000)

Como se puede observar la clasificación se basa en el número de empleados y lo que consideramos, en general pequeña empresa la subdivide en micro y pequeñas, según el número de empleados que se expone en la tabla. Se completa con las medianas y grandes empresas.
A continuación exponemos la clasificación de la **Unión Europea (UE)** que tiene en cuenta más criterios, además del número de trabajadores, tal y como se puede ver en la Tabla. En este caso, se tiene en cuenta además, el volumen de negocio y el balance general de la empresa.

Tabla 2. Clasificación de empresas según la UE

Categoría de empresa	Efectivos	Volumen de negocio	Balance general
Mediana	<250	<= 50 millones EUR	<= 43 millones EUR
Pequeña	<50	<= 10 millones EUR	<= 10 millones EUR
Micro	<10	<= 2 millones EUR	<= 2 millones EUR

La definición de estos criterios, también está recogida en el **Anexo I del Reglamento (UE)** nº 651/2014 de la Comisión. Para poder adscribir a una empresa a una categoría debe cumplir el requisito de los efectivos y como mínimo uno de los otros dos. Para facilitar este trabajo a las empresas, la UE ha puesto a su disposición la herramienta soypyme que se encarga de automatizar el proceso de cálculo.

Este último criterio es el más extendido, pero en España hay dos puntos de vista más para poder clasificar las empresa como PYME, el punto de vista contable, el cual juzga si una empresa puede acogerse al plan general contable especial para PYMES y el punto de vista fiscal que estima si la empresa puede acogerse a un régimen especial en el Impuesto sobre sociedades. Ambos criterios quedan recogidos respectivamente en las tablas siguientes

Tabla 3.- Empresas que pueden acogerse al plan general contable o al Impuesto de sociedades

Tamaño	Activo	Facturación	Trabajadores
PYME	<= 2850000	<= 5700000	< 50
Grande	> 2850000	> 5700000	> 50

Tamaño	Facturación
PYME	<10000000
Grande	<10000000

Y a título informativo, añadimos que a día 1 de enero de 2018 el DIRCE (directorio central de empresas) registra 3.337.646 empresas con actividad en España. Disgregando según el número de empleados, el 95,4% del total son microempresas, mientras que las pequeñas y medianas empresas ocupan un 3,8% y un 0,6% respectivamente. Finalmente las Grandes empresas ocupan el 0,2% restante.
Por lo que podemos decir, que la economía española está formada en su gran mayoría por las PYMES.
Además, podemos concluir que los distintos elementos analizados para clasificar las empresas según la OCDE, la UE o los planes contables o Impuestos de sociedades, no nos parecen contradictorios, sino más bien complementarios y responden a criterios más o menos unificados.

2.1.2. A nivel internacional.

Finalmente con el objetivo de dotar de una mayor perspectiva al trabajo se procede a dar una somera visión del concepto de PYME alrededor del mundo.

a) En el continente americano, distinguimos entre América del Norte y América del Sur.

En América del Norte, tomamos como referencia a Estados Unidos, donde se consideran como principales criterios para su clasificación el número de empleos y el monto de capital, según se muestra en la tabla adjunta.

Tabla 4. Clasificación de empresas en los Estados Unidos

Tamaño	Número de empleos	Monto de capital
Micro	< 100	5 a 6 millones de dólares
Pequeña	100	Cifra de participación
Mediana	>100 y < 250	

Fuente: Elaboración en base a Villegas (2012).

Respecto a América latina podemos decir que, no existe una definición homogénea del término por lo que en cada país se le da un enfoque diferente, en la tabla que se muestra a continuación se ilustran las distintas realidades en Chile, Guatemala, México, Panamá y Uruguay.

Tabla 5. Clasificación comparativa de empresas en distintos países de América latina

	Chile (ventas)	Guatemala (Empleo)	México (Empleo)	Panamá (Ingresos Brutos)	Uruguay (Empleo)
Micro	Hasta 58	Hasta 10	Hasta 10	Hasta 150	Hasta 4
Pequeña	Hasta 600	Hasta 25	Hasta 50	Hasta 1000	Hasta 19
Mediana	Hasta 2400	Hasta 60	Hasta 250	Hasta 2500	Hasta 99
Grande	+ de 2400	+ de 60	+ de 250	+ de 2500	+ de 99

Fuente: Elaboración Propia. (1) Servicios de Impuestos internos, 2003, INE y MIDEPLAN (2) Instituto de Estadística (INE), Censo Industrial 1999. (3) INEGI. (4) Directorio de establecimientos, Contraloría General de la República, 1998. (5) Observatorio PYME Uruguay.

Como se puede observar los distintos países utilizan distintos estándares para su clasificación aunque se ha intentando unificar la comparativa con los mismos criterios: ventas, empleo e ingresos brutos pero la diversidad y disparidad es la norma.

b) En el continente asiático nos centraremos en Japón y China,

En ambos países cuentan con la particularidad que los mínimos y máximos para clasificar una empresa como PYME dependen del sector en el que opere.

En Japón, destacan los sectores de: manufactura, construcción y otros, el intermediario, los servicios y los minoristas y dentro de ellos centran su interés en criterios como el capital o los empleados permanentes.

Tabla 6. Clasificación de empresas por sectores de producción en Japón

	Micro Empresas		
	Capital	Empleados permanentes	Empleados permanentes
Manufactura, Construcción, otros	Menos de 3.2 millones de USD	Menos de 300 empleados	Menos de 20 empleados
Intermediario	Menos de 1 millón de USD	Menos de 100 empleados	Menos de 5 empleados
Servicios	Menos de 540 mil de USD	Menos de 50 empleados	
Minoristas			

Fuente: Libro Blanco de PYMES, Ministerio de Economía e Industria de Japón.

En China, destacan los sectores de: industria, construcción, comercios minoristas y mayoristas, transporte, correos y comunicaciones y hoteles y restaurantes y dentro de ellos los criterios preferentes son: el tamaño de la empresa, el número de empleados, el volumen del negocio y el total del balance, tal y como se puede observar en la tabla adjunta.

Tabla 7. Normativa para la definición de las PYMES en China

Sector	Tamaño de la empresa	Número de empleados	Volumen de negocios (miles de yuanes)	Total del balance (miles de yuanes)
Industria	Mediana	300 – 2000	30000 – 300000	40000 – 400000
	Pequeña	< 300	< 30000	< 40000
Construcción	Mediana	600 – 3000	30000 – 300000	40000 – 400000
	Pequeña	< 600	< 30000	< 40000
Comercio minorista	Mediana	100 – 500	10000 – 150000	
	Pequeña	< 100	< 10000	
Comercio mayorista	Mediana	500 – 3000	30000 – 300000	
	Pequeña	< 500	< 30000	
Transporte	Mediana	500 – 3000	30000 – 300000	
	Pequeña	< 500	< 30000	
Correos y comunicaciones	Mediana	400 – 1000	30000 – 300000	
	Pequeña	< 400	< 30000	
Hotel y restaurantes	Mediana	400 – 800	30000 – 150000	
	Pequeña	< 400	< 30000	

Fuente: Normativa para la definición de las PYME (2003). Tomado de Yu et al; 2003. 1.000 yuanes = 100 euros

Observar que el sector "hoteles y restaurantes" el número de empleados que la define es de los más pequeños entre 400 y 800 trabajadores, mientras que en los sectores de comunicación, comercio mayorista y transporte puede llegar a los 3000 trabajadores. Respecto al volumen de ventas se encuentra entre los más bajos, equiparado en parte con el sector del comercio minorista.

Llegados a este punto del análisis, y al realizar una breve comparativa en el ámbito internacional sí que encontramos diferencias significativas en cuanto a las clasificaciones de empresas.
En América del Norte, aunque la terminología (ej: monto de capital) puede variar, se asemeja en cierta manera a la europea, mientras que en América del Sur, no existe ningún tipo de uniformidad, de hecho cada país revisado, no sólo utiliza distintos criterios comparativos, sino que ante criterios más o menos unificados los intervalos numéricos también están poco consensuados.
Y en el continente asiático, tal vez lo más diferente sea el hecho de que se clasifican las empresas, además del tamaño, número de empleados, volumen de facturación...por el sector al que representan. Y mientras en Japón encontramos el sector "servicios" donde se incluiría el objeto de este trabajo, en China, define un sector específico para "hotel" aunque se encuentra compartido con restaurantes.

2.2. Las PYMES en España.

Después de haber definido de forma genérica el concepto de PYMES y revisar las variaciones que surgen en Europa y en otras partes del mundo acerca del concepto, hemos llegado a la conclusión que en España el concepto de PYMES es el mismo que se recoge en la Unión Europea. Incluye a las empresas: micro, pequeñas y medianas y las definen: el número de empleados, los efectivos, el volumen de negocio y el balance general, como elementos clave.
Pero la definición de PYME, también distingue otros tipos de empresa en función del tipo de relación que mantiene con otras empresas, respecto a participación en el capital, el derechos de voto o el derecho a ejercer una influencia dominante. Esto nos lleva a una nueva clasificación del tipo de empresas.

2.2.1.- Tipos de empresas según los niveles de participación

Según el nivel de participación se distinguen tres tipos de empresa:

Tabla 8: Tipos de empresa según niveles de participación

Tipo de empresa	Definición	Características
AUTÓNOMA	Es el caso más frecuente. Se considera así, si no es ni asociada ni vinculada.	1. No poseer una participación igual o superior al 25% en otra empresa. 2. El 25% o más de la empresa, no es propiedad de otra u otras empresas u organismos 3. No elabora cuentas consolidadas ni se incluye en las cuentas consolidadas de otra empresa que las realice y por lo tanto no es una empresa vinculada.
ASOCIADA	Mantienen relaciones de asociación financiera con otras empresas, aunque ninguna ejerza un control efectivo sobre la otra. Son asociadas, las empresas que no son autónomas, ni están vinculadas entre sí.	1. Poseer una participación en dicha empresa entre el 25% y el 50%. 2.- Posee una participación comprendida entre el el 25% y el 50% de dicha empresa 3.- No elabora cuentas consolidadas por consolidación, ni está incluida en las cuentas de la empresa ni de las vinculadas a ella.
VINCULADA	Son casos menos habituales Y por eliminación es, vinculada, cuando no se cumple las características ni de autónoma ni de vinculada.	1.- Empresas que forman parte de un grupo que controla directa o indirectamente, la mayoría de su capital o derechos de votos. 2. El control se realiza a través de acuerdos o de personas físicas accionistas. 3.- Está sujeta a la obligación de elaborar cuentas consolidadas o está incluida por consolidadas en las cuentas de una empresa obligada a elaborar cuentas consolidadas.

Cuadro de elaboración propia a partir de las definiciones

El tipo de empresas vinculadas con el sector hotelero son en su mayoría, autónomas o asociadas.

2.2.2 Ideas sobre la normativa básica para el desarrollo de las PYME en España

Para el conocimiento de las PYME en España y antes de pasar a sus obligaciones consideramos incorporar unas breves ideas de las referencias normativas, recogidas en la página web del Ministerio de Industria, Comercio y Turismo, dentro de la Dirección General de Industria y de la Pequeña y Mediana Empresa y concretamente en el portal "PYMES". No realizaremos un estudio exhaustivo, sólo unas breves pinceladas para enmarcar el estudio a realizar y el conocimiento de las PYME. Hemos evitado, la relación normativa de tipo jurídico, para centrarnos en los temas que se regulan en la normativa.

En primer lugar, nombraremos unos elementos básicos de carácter general que afectan también a las PYME:

- Tratamiento y protección de datos personales y libre circulación de estos datos.
- Garantía de los derechos digitales.
- Normativa de Administración Electrónica.
- Consejo Estatal de la pequeña y mediana empresa.
- Ley de Economía Sostenible.
- Reglamento del Registro Mercantil
- Creación de la ventanilla única de la Directiva de servicios en los puntos de atención al Emprendedor.
- Y, actuaciones en el ámbito fiscal, laboral y liberalizadoras para fomentar la inversión y la creación de empresas.

En segundo lugar, nos centraremos en las ideas básicas de creación de empresas, creación de empresas por internet y cese de empresas. Destacamos las siguientes ideas clave que están reflejadas en la normativa:

- Sociedades laborales y participadas.
- Reglamento de las empresas de trabajo temporal.
- Derechos de los accionistas de sociedades cotizadas.
- Ley de Sociedades de Capital.
- Ley del Estatuto del trabajo autónomo.
- Ley de Sociedades profesionales.
- Regulaciones específicas y condiciones para el empleo del Documento Único Electrónico (DUE) para la puesta en marcha de sociedades cooperativas, sociedades civiles, comunidades de bienes, sociedades limitadas laborales y emprendedores de responsabilidad limitada mediante el sistema de tramitación telemática.
- Regulaciones para el cese de actividad de las empresas individuales.

En tercer lugar, desarrollaremos las condiciones normativas que regulan el mundo de los emprendedores y PYME, así como la innovación :

- Reformas del trabajo Autónoma.
- Reglamento de las empresas de trabajo temporal
- Mecanismos de segunda oportunidad, reducción de carga financiera y otras medidas.
- Medidas urgentes para el crecimiento, la competitividad y la eficiencia.
- Leyes de apoyo a los emprendedores y su internalización, así como de estímulo del crecimiento y de la creación de empleo.
- Regulación del Registro de la pequeña y mediana empresa innovadora, así como la obtención del sello de pequeña y mediana empresa innovadora.

En cuarto lugar, nos centraremos en el ejercicio de la actividad empresarial. En este apartado se desarrollan los mecanismos fundamentales para la organización y funcionamiento de los PYMES:

- Ley General de la Seguridad Social.
- Reglamento de los Servicios de Prevención.
- Ley por la que se actualiza la normativa en materia de autoempleo y se adoptan medidas de fomento y promoción del trabajo autónomo y de la Economía Social.
- Ley de fomento de la financiación empresarial.
- Condiciones técnicas y funcionales que debe reunir el Punto General de Entrada de Facturas Electrónicas.
- Medidas urgentes en materia de refinanciación y reestructuración de deuda empresarial.
- Regulación del contenido de los contratos de trabajo.
- Ley sobre modificaciones estructurales de las sociedades mercantiles.
- Resolución sobre el Libro de Visitas electrónico de la Inspección de Trabajo y Seguridad Social.
- Plan General de Contabilidad de Pequeñas y Medianas Empresas y los criterios contables específicos para microempresas.
- Plan General de Contabilidad.
- Servicios de la sociedad de la información y de comercio electrónico.

En quinto lugar, citaremos algunas de las medidas fiscales básicas a las que están sujetas la PYMES en nuestro país:

- Reglamento del Impuesto sobre Sociedades.
- Normas para la gestión del Impuesto de Actividades Económicas
- Reglamento sobre el Impuesto de Valor Añadido.
- Impuesto sobre la renta de las personas físicas, medidas urgentes para reducir su carga tributaria.
- Reglamento de Planes y fondos de pensiones.

Y por último, incluimos unas breves referencias respecto a la normativa laboral:

- Ley de Empleo.
- Condiciones generales de la contratación.
- Texto refundido de la Ley del Estatuto de los Trabajadores.
- Medidas urgentes para el fomento del empleo y la contratación indefinida.
- Medidas urgentes para la reforma del mercado laboral

En este apartado hemos tratado de dar una visión organizada sobre la puntos básicos que regulan la organización y funcionamiento de los PYMES en España, sin entrar en ninguna normativa específica y menos en su desarrollo. Para ello, hemos enumerado los elementos de carácter general que afectan al sistema productivo español, desde la Administración electrónica, la protección de datos o las medidas para la fomentar la creación de empresas. Apartado este último que le hemos dado punto específico, dada su trascendencia.
También hemos querido subrayar el mundo de los emprendedores que tan condicionantes son en el mundo laboral y por tanto en las PYMES y siempre vinculandolo a la innovación y empresa innovadora.
Pero ha sido en los apartados cuarto y quinto dónde hemos enumerado lo necesario para el desarrollo de la actividad empresarial desde la seguridad social, el plan de contabilidad, la facturación electrónica o los impuesto específicos: sociedades, Impuesto de Actividades Económicas, o Impuesto de valor añadido.
Para terminar hemos querido incluir, la importancia de la creación de empleo, los mecanismos para la contratación o el mismo estatuto de trabajadores, que tanto condicionan en cualquier sector de producción y por supuesto en el de "hoteles".

2.2.3. Obligaciones y otras consideraciones de las PYME en España.

La realización de una actividad económica da lugar al cumplimiento de unos trámites administrativos que, a su vez, originan unas obligaciones que el empresario debe cumplir. Siguiendo la página web del Ministerio, en su portal PYMES podemos decir que las obligaciones de las PYMES en España, se pueden dividir en dos fundamentalmente: obligaciones fiscales y obligaciones contables. Ambas han estado enumeradas en el punto anterior con otros criterios pero ahora las vamos a especificar concretamente:

a) Obligaciones fiscales

Entre las obligaciones fiscales de obligado cumplimiento están:

- Impuesto sobre la Renta de las Personas Físicas (IRPF), con carácter anual y con la posibilidad de pago fraccionado
- Impuesto sobre Actividades Económicas (IAE), en la que se exige la comunicación del importe neto de la cifra de negocios. Puede suponer también la declaración de alta, baja o variación de actividades económicas.
- Impuesto sobre el Valor Añadido (IVA). Suponen liquidaciones del impuesto y resúmenes anuales.
- Obligaciones de facturación. Tener en cuenta el tipo de factura: normal, simplificada, rectificada o electrónica. Obligación de conservarlas para cumplir con sus obligaciones tributarias.
- Retenciones e ingresos a cuenta
- Comunicaciones y notificaciones por medios electrónicos
- Inclusión en el censo de empresarios y profesionales
- Declaraciones Intrastat si se dedica a la importación, exportación
- Otros trámites: declaración anual con terceras personas o comunicación de datos al pagador- retenciones sobre rendimientos del trabajo.

b) Obligaciones contables

Respecto a las obligaciones contables destacamos:

- Libros contables. Destacan el libro diario, los libros de ventas/ingresos, de compras/gastos y los libros de facturas expedidas, recibidas…
- Cierre del ejercicio del Empresario Responsabilidad Limitada: libros de inventarios y cuentas anuales y aprobación de las mismas
- Obligaciones registrales. Depósito de las cuentas en el registro mercantil y legación del libro diario y del libro de inventarios y cuentas anuales

Y por último añadir otra básica, las relacionadas con la Seguridad Social, para ello, hemos tenido en cuenta las aportaciones de sendos artículos en web, uno de astac.com que nos acerca a las obligaciones de los empresarios en materia de seguridad social y en el otro publicado en el País Economía por Teresa Álvarez, que completa las obligaciones de las PYMES en materia de desempleo.

c) Obligaciones con la Seguridad Social

Cotizar a la Seguridad Social por los trabajadores que tiene a su cargo, es la primera. O sea su afiliación, así como comunicar las variaciones de los trabajadores.

- En relación a los conceptos y cuantía por los que se debe cotizar, se pueden distinguir diferentes conceptos: contingencias comunes, horas extraordinarias, contingencias profesionales: Incapacidad temporal (IT) o Invalidez, Muerte y supervivencia (IMS) y otras cotizaciones: desempleo, fondo de garantía salarial y formación profesional.
- En cuanto al desempleo, la Pyme está obligada a cumplir una serie de requisitos, para asegurar que los trabajadores, en el caso de quedarse sin empleo, tengan acceso a paro. Y eso genera la siguientes obligaciones:
    - Cotizar a la contingencia de desempleo
    - Proporcionar información y documentación relativa al reconocimiento, suspensión o reanudación del derecho a las prestaciones.
    - En los casos de los expedientes para la regulación de empleo tienen que realizar el pago delegado de las prestaciones de desempleo.
- El Fondo de Garantía Salarial (FOGASA) es un organismo cuya finalidad es el abono a los trabajadores, previa instrucción de expediente , del importe de los salarios pendiente de pago, a causa de insolvencia, suspensión de pagos, quiebra o concurso de acreedores.

Llegados a este punto y después de ver que las PYMES pueden tener distintos niveles de participación, están organizadas por una normativa extensa que desarrolla un gran número de temáticas expuestas con anterioridad y después de comprobar cuales son sus obligaciones, nos planteamos si tiene más ventajas o inconvenientes considerarse una PYME. Vamos a tratar de definir, ahora y para finalizar, cuáles son las principales ventajas e inconvenientes en el caso de las PYMES

Algunas ventajas

- Acceso a subvenciones y ayudas. La financiación es una de las grandes barreras de las pymes. Para contrarrestarlo, existen multitud de líneas de ayuda.
- Flexibilidad. Se pueden adaptar con más rapidez a los cambios del mercado. Pueden incluso modificar su actividad, algo impensable en una gran marca.
- Proximidad y trato personalizado. En muchos sectores, los clientes agradecen el trato personalizado. En la mayor parte de las pymes, sobre todo las "micro" y pequeñas empresas, son los propios empresarios los que tratan con el cliente.
- Cohesión en la dirección y compromiso de los trabajadores. La unidad de mando es total y los vínculos que se establecen entre empleados y empresarios son más cercanos, lo que aumenta el compromiso de la plantilla.

También por causa de su tamaño y de su reducido volumen de negocio, una pyme tiene una **serie de desventajas** frente a las grandes empresas.

- Impacto del entorno económico. Una pyme tiene menos margen de acción ante factores como la inflación o la deflación.
- Escasa capacidad de negociación ante grandes proveedores y/o distribuidores.
- Fuentes de financiación reducidas. El acceso al crédito limitado es la gran barrera de las pymes. Menor financiación significa menor capacidad de inversión en desarrollo, innovación o formación y actualización de la plantilla. (inversión limitada en I+D)
- U otros factores, como las dificultades para mantener su credibilidad o elevar los niveles de productividad.

Y su digitalización es también uno de los grandes desafíos en todos los sectores productivos y en especial, en el sector turístico y hotelero uno de los sectores más potentes, hasta ahora en nuestro país. Y terminamos con una firme convicción que las pequeñas y medianas empresas son y continuarán siendo esenciales en el día a día de la economía española y europea.

2.3. Niveles de Informatización de las PYMES españolas

Para hablar sobre las distintas tipologías de implantaciones informáticas en las PYMES españolas debemos analizar los 5 niveles de informatización de las TIC que nos ofrece el informe E-PYME 2018 en el que se realiza un análisis sectorial de la implantación de las TIC en las empresas españolas. En los distintos niveles se han seleccionado los indicadores que se considera tienen mayor relación con el objeto del trabajo.
En primer lugar, procedemos a nombrar cada uno de los niveles junto con los indicadores seleccionados:

1. Infraestructuras básicas que permiten el acceso a Internet
   Indicadores seleccionados:
   - Uso de ordenadores
   - Conexión a Internet

2. Presencia y los usos de Internet por parte de las empresas
   Indicadores seleccionados:
   - Disponibilidad de página web
   - Presencia a través de medios sociales
   - Interacción con las Administraciones Públicas a través de medios telemáticos

3. Comercio electrónico
   Indicadores seleccionados:
   - Compras realizadas a través de Internet
   - Ventas realizadas a través de Internet

4. Integración por parte de las empresas de tecnologías clave
   Indicadores seleccionados:
   - Cloud Computing
   - Uso de herramientas en materia de ciberseguridad

5. Talento digital en las empresas
   Indicadores seleccionados:

- Presencia de especialistas en materia de TIC
- Impartición de actividades formativas en TIC al personal

Una vez presentados los distintos niveles de informatización y los indicadores seleccionados procedemos a analizar con detalle cada uno de ellos. Cada análisis se acompaña con una gráfica que desglosa los datos ofrecidos en los principales sectores, a saber:

- Industria
- Construcción
- Venta y reparación de vehículos de motor
- Comercio al por mayor
- Comercio al por menor
- Hoteles y agencias de viaje
- Transporte y almacenamiento
- Información y comunicaciones
- Actividades inmobiliarias, administrativas y servicios auxiliares
- Actividades profesionales, científicas y técnicas

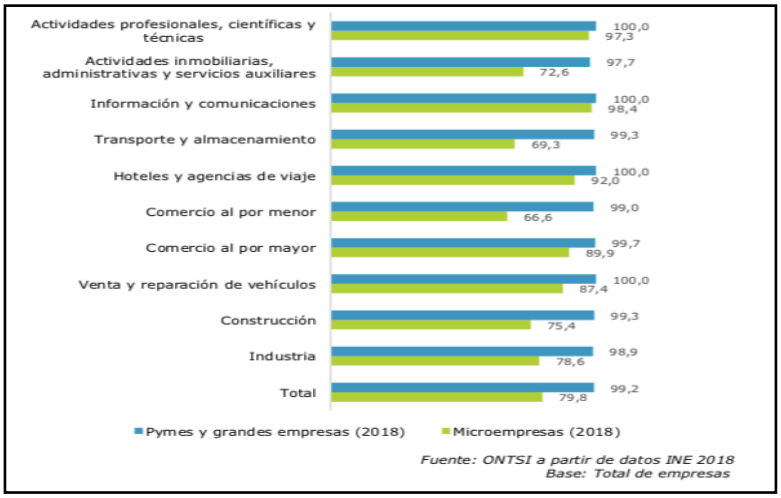
Así pues, la metodología a utilizar en este punto consiste en analizar brevemente los 5 niveles de informatización de las TIC, seleccionando los indicadores de cada nivel, más significativos para nuestro trabajo. Se estudiarán a través de unas tablas extraídas del ONTSI (Observatorio nacional de las telecomunicaciones y de la sociedad de la información). Y finalmente nos centraremos en el sector específico de "hoteles y agencias de viaje" que es el objeto de estudio.

- Infraestructuras básicas que permiten el acceso a Internet

- **Uso de ordenadores**

Con carácter general y según el estudio realizado en 2018, se puede afirmar que prácticamente la totalidad de las compañías de 10 trabajadores o más dispone de ordenadores (99,2%). Entre las empresas de menos de 10 empleados el porcentaje se sitúa en un 79,8%.

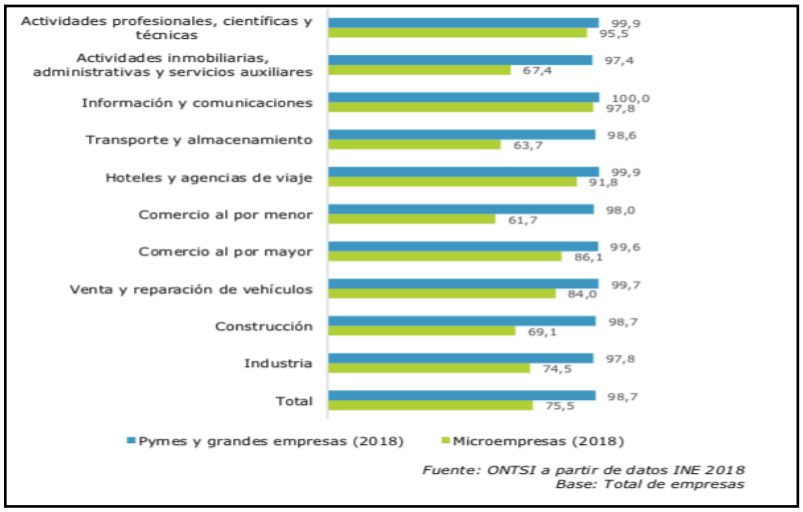
Tabla 9.- Uso de ordenadores



- **Conexión a Internet**

En el caso de conexión de la internet el porcentaje de PYMES y grandes empresas se aproxima al 99%. Sin embargo, en las microempresas, la cifra se sitúa en un 75,5%

Tabla 10.- Conexión a internet



Se puede concluir que el uso de ordenadores y la conexión a internet en las PYMES y grandes empresas están prácticamente generalizadas por lo que las estructuras básicas de acceso a internet, están garantizadas. Sólo en las microempresas se aprecian resultados más bajos.

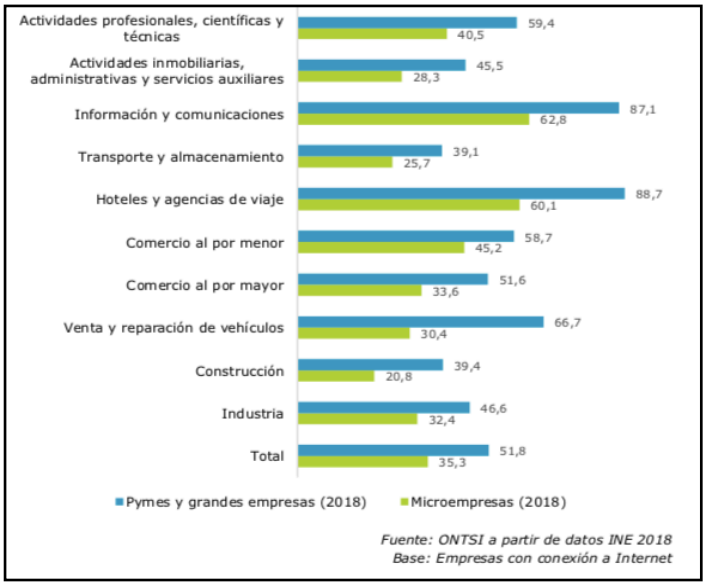
El sector "hoteles y agencias de viaje" se encuentra en los primeros lugares sólo por debajo del sector de información y de actividades científicas y técnicas, tanto en PYMES y grandes empresas como en las microempresas. En estas últimas, la conexión a internet, es ligeramente inferior y podemos pensar que se debe a las dificultades de conexión en el ámbito rural. Pero en ambos indicadores se sitúan significativamente por encima de la media. Por ello, podemos afirmar que los hoteles son entornos con buenas dotaciones de ordenadores y con una alta accesibilidad a internet, en el caso de nuestras PYMES.

- **Presencia y uso de Internet**

- **Disponibilidad de página web**

En 2018, el 78,2% de las compañías de 10 o más trabajadores y el 31,1% de las microempresas disponían de página web corporativa**.**

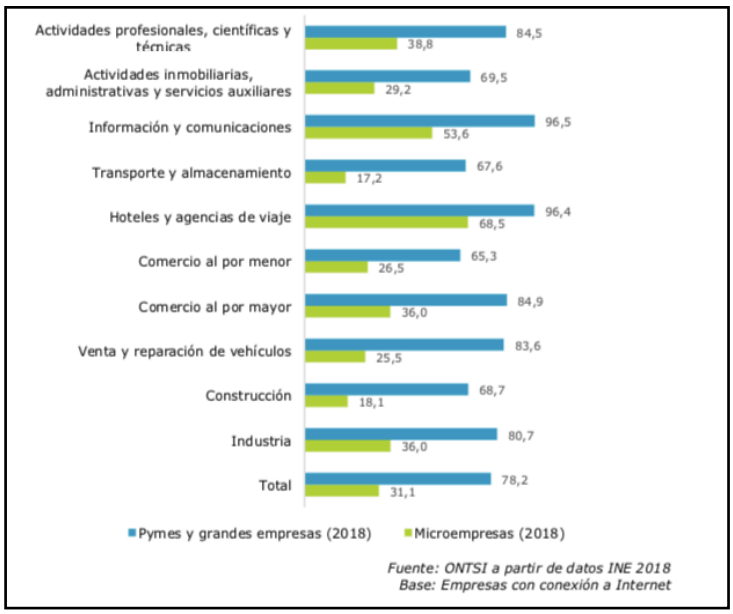
Tabla 11. Disponibilidad de página web



- **Presencia a través de medios sociales**

El uso de medios sociales con fines corporativos no se ha extendido tanto como el uso de páginas web, al menos en el caso de las PYMES y grandes empresas. Así, en 2018, un poco más de la mitad de las empresas de 10 o más empleados utiliza medios sociales y a su vez un 35,3% de las microempresas españolas también lo hace.

Tabla 12. - Presencia a través de medios sociales

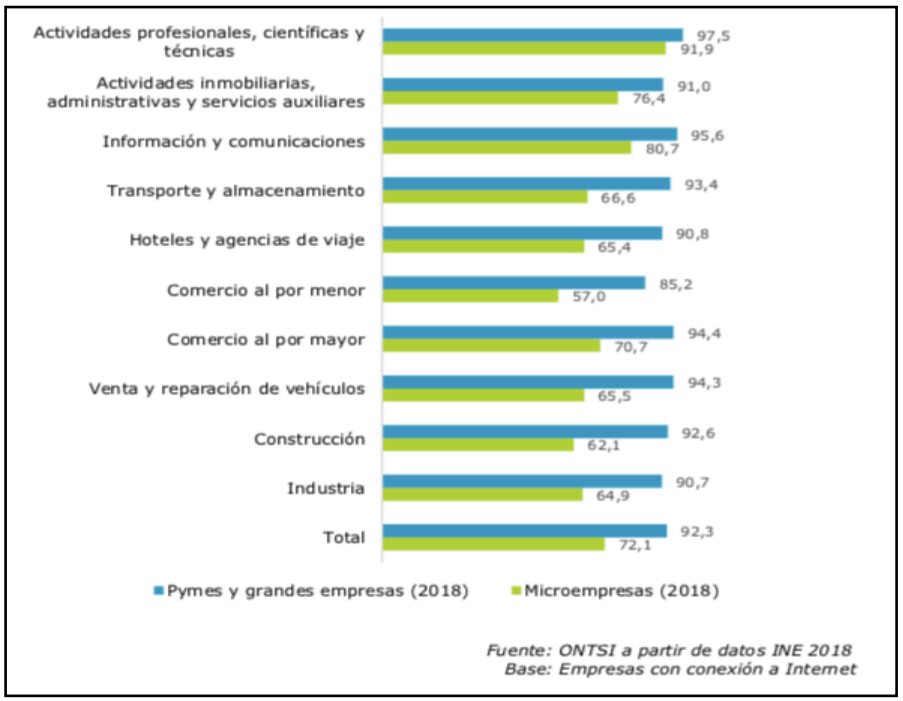


- **Interacción con las Administraciones Públicas a través de medios telemáticos**

El número de compañías que **interactuó con la Administración Pública** por medios telemáticos se sitúa en el 92,3% para las PYMES y grandes compañías y el 72,1% para las microempresas.

Al interpretar los resultados expresados en el siguiente gráfico, se debe matizar que, de conformidad con lo dispuesto en el artículo 14 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, están obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas las personas jurídicas, las entidades sin personalidad jurídica y quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración. El que no se alcance en ningún caso el 100% de las empresas se debe a que muchas de ellas, sobre todo las microempresas, mantienen estas relaciones a través de terceros o representantes.

Tabla 13.- Interacción con las Administraciones Públicas a través de medios telemáticos



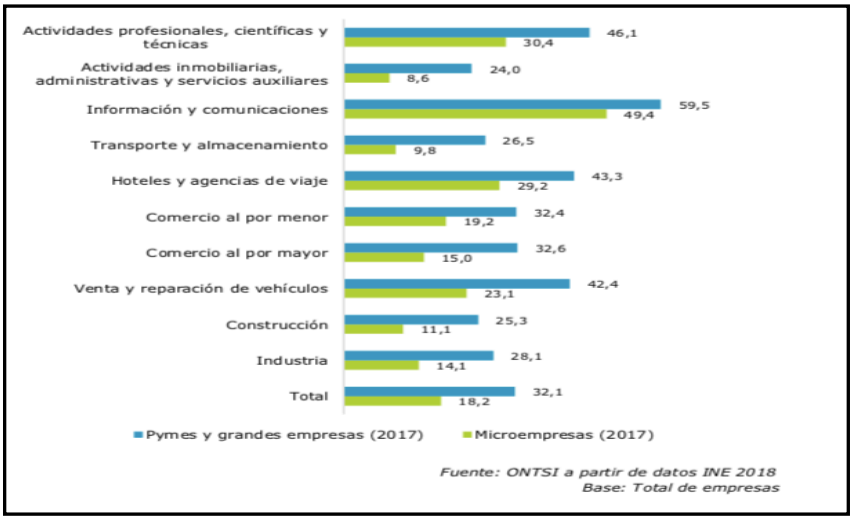
En cuanto a la presencia y uso de internet en los hoteles y agencias de viajes, podemos decir que está prácticamente implantado como en la mayoría de los sectores. Destaca el 96,4% de la presencia a través de medios sociales, al mismo nivel que el sector información y comunicaciones y le supera en el caso de la disponibilidad de página web, siempre en el caso de las PYMES y grandes empresas.
Respecto a la interacción con las Administraciones Públicas, a través de medios electrónicos, aunque el porcentaje es alto, se sitúa en los últimos lugares junto con el sector de la industria, aunque hay que subrayar que las diferencias se reducen a escasos puntos.
Así pues, podemos afirmar que en las PYMES, tienen una alta disponibilidad de páginas web, que su presencia a través de medios sociales está consolidada y que para los trámites con la Administraciones Públicas, ya se utiliza de forma generalizada, los medios electrónicos.

. Comercio electrónico

- **Compras realizadas a través de Internet**

El 32,1% de las PYMES y grandes empresas y el 18,2% de las empresas de menos de 10 trabajadores adquirieron productos o servicios a través de Internet.

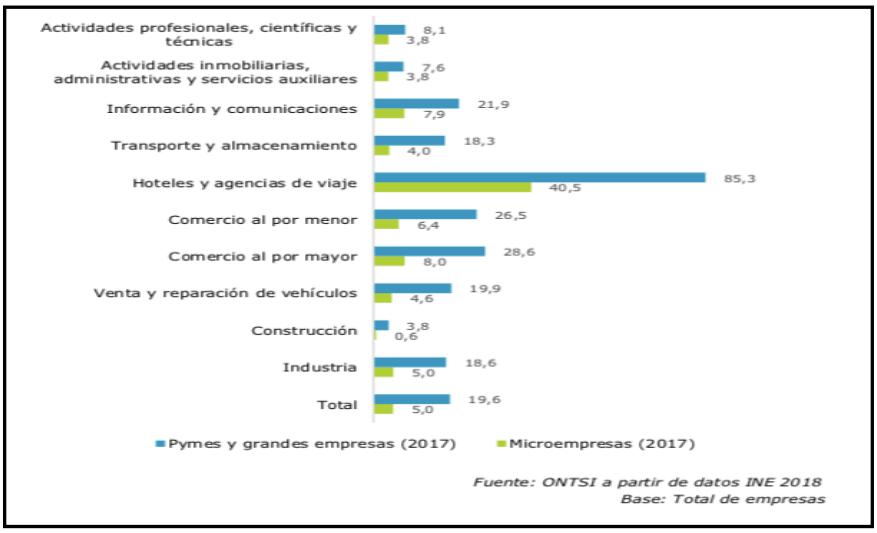
Tabla 14.- Compras realizadas por internet



- **Ventas realizadas a través de Internet**

El porcentaje de microempresas que realizó **ventas por comercio electrónico** fue del 5%, proporción que entre las PYMES y grandes compañías asciende hasta el 19,6%.

Tabla 15.- Ventas realizadas a través de internet



Respecto al comercio electrónico, podemos apreciar una diferencia muy significativa entre las compras y las ventas realizadas por internet. Las primeras se encuentran en unos niveles similares a los sectores que las utilizan en el caso de las PYMES. Pero es en el apartado de las ventas realizadas a través de internet donde encontramos una diferencia muy significativa de más de 50 puntos en el caso de las pymes pero también es muy alta respecto al resto de los sectores en el caso de las microempresas.

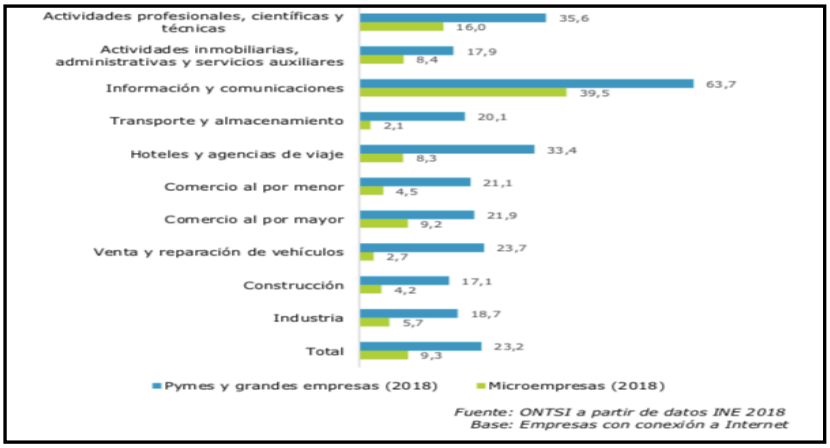
Podemos pues afirmar, que las ventas realizadas a través de internet es uno de los puntos fuertes del sector hoteles y agencias de viajes

Uso de tecnologías clave

- **Cloud Computing**

La utilización de herramientas de Cloud Computing todavía, en 2018, no se ha extendido significativamente entre el tejido empresarial español. Si se atiende al total nacional, sólo un 23,2% de las PYMES y grandes compañías y un 9,3% de las microempresas compró algún servicio de Cloud Computing usado a través de Internet.

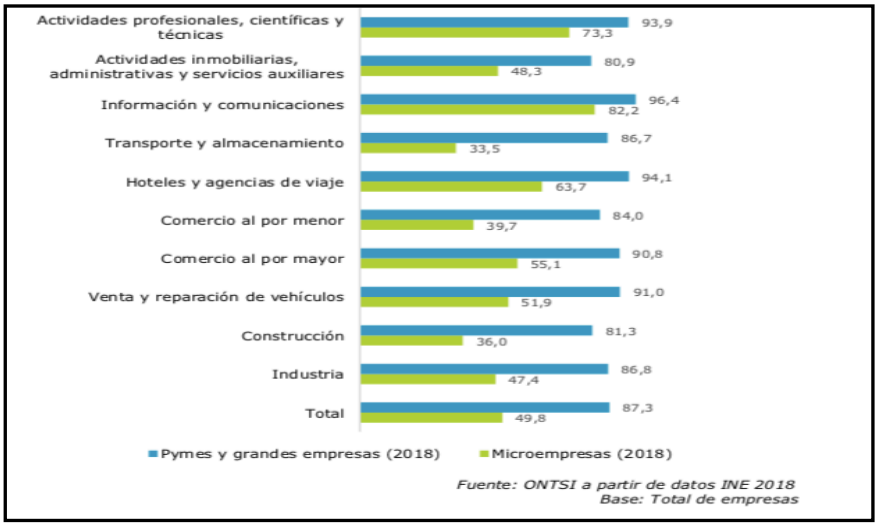
Tabla 16.- Cloud Computing



- **Uso de herramientas en materia de ciberseguridad**

Con respecto a los sistemas internos de ciberseguridad, el 87,3% de las PYMES y grandes compañías y el 49,8% de las microempresas hicieron uso de ellos en 2018.

Tabla 17.- Uso de herramientas en materias de ciberseguridad



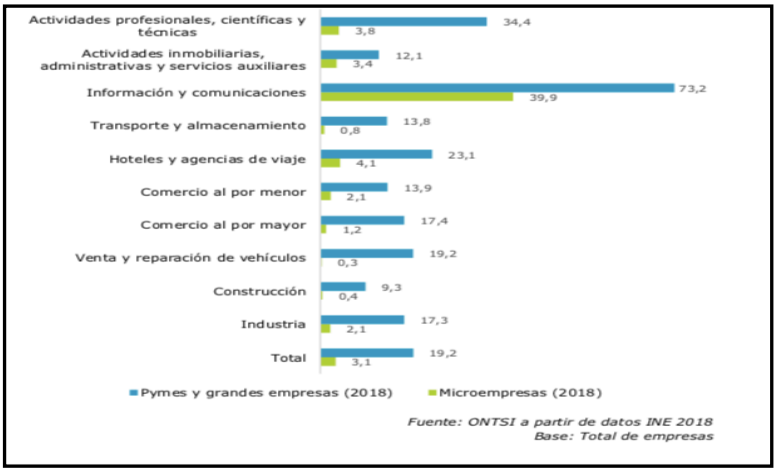
Por sectores de actividad económica, en todos los casos, en las PYMES y grandes empresas se observa un escaso uso de herramientas de cloud computing, sólo destaca el sector de información y comunicaciones. Podemos asegurar, por tanto, que es uno de los factores más débiles de los niveles de informatización de las PYMES españolas. En cambio, el uso de herramientas de ciberseguridad, si está altamente desarrollado sobre todo en los pymes y grandes empresas, destacando los sectores de información y comunicaciones y los hoteles y agencias de viaje, que se sitúa en el segundo lugar de uso, demostrando el interés del sector en el uso de estas herramientas.

Talento digital

- **Presencia de especialistas en materia de TIC**

La presencia de especialistas en materia de TIC constituye un aspecto que viene determinado fundamentalmente por el tamaño de las empresas, pero también por el tipo de actividad que realizan. En términos globales, el 19,2% de las PYMES y grandes compañías cuenta con empleados con este perfil. Por el contrario, el porcentaje de microempresas se reduce a tan solo un 3,1%.

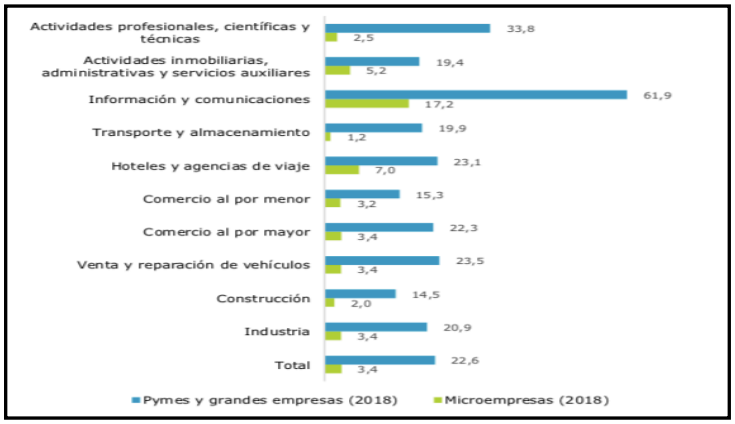
Tabla 18.- Presencia de especialistas en materia de TIC



- **Impartición de actividades formativas en TIC al personal**

Finalmente, el 22,6% de las PYMES y grandes empresas y solo el 3,4% de microempresas facilitaron actividades formativas en TIC. En la mayor parte de los casos, las actividades se orientaron fundamentalmente al personal no especialista en TIC (84,4% en las PYMES y grandes empresas, y 77,8% en las microempresa).

Tabla 19.- Impartición de actividades formativas en TIC al personal



Aunque consideramos que la existencia de especialistas TIC, al igual que la formación en materia de TIC, es condicionante en cualquier sector económico, podemos observar que estos aspectos no están nada desarrollados en España. En el caso de especialistas se entiende en el caso de empresas con poco personal pero la formación en actividades TIC debería ser obligatoria, no sólo como requisito de acceso al puesto de trabajo sino también por el hecho de una actualización permanente de herramientas informáticas. Los sectores en que está más desarrollado son: información y comunicaciones, actividades profesionales, en el caso de personal TIC y en el caso de formación, estos sectores se encuentran en los mismos primeros lugares, seguidos por la agencia de viajes, comercio al por mayor, ventas de automóviles e industria.

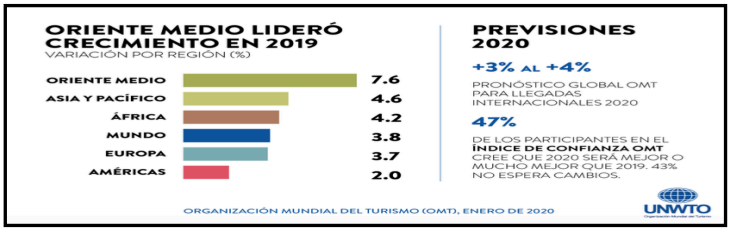
3.- INTRODUCCIÓN AL SECTOR TURÍSTICO

El turismo en una economía es uno de los sectores que genera mayores ingresos y fuentes de trabajo, tanto directas como indirectas, en pequeñas y medianas empresas (PyMES). A través de ellas se fortalecen sus ingresos y la distribución de la riqueza, aspectos fundamentales para el crecimiento económico de las naciones. Para muchos países en desarrollo, el turismo se ha convertido en una estrategia para desarrollar el sector servicios. Es importante considerar que el desarrollo de la actividad turística está en relación directa con el nivel de ingresos, y su efecto multiplicador en comparación con otros sectores productivos tradicionales es muy amplio, por los beneficios directos (generación de riqueza) e indirectos (empleo y gastos derivados sobre otros sectores productivos).

3.1.- El sector turístico en en la economía internacional

Según los datos ofrecidos por el informe anual del World Travel & Tourism Council (WTTC), el sector del turismo es el 4º sector con mayor impacto en el PIB mundial, tan solo superado por los sectores mineros, agrícola y automotriz, representando un 10,3% del PIB mundial. En 2019 fue el generador de 1 de cada 10 puestos de trabajos.
La industria de los viajes y el turismo generó un impacto económico directo de 2,4 billones de dólares el año pasado, lo que representa un 3,1% del PIB mundial. Pero si se suman los efectos directos e indirectos, el turismo genera el 9,8% de la producción económica mundial. Así, considerando el impacto económico total, el turismo supera otros sectores como la industria química (8,6%), la agricultura (8,5%), la educación (8,4%), la automoción (7%) o la banca (5,9%).
La última investigación anual de WTTC, en conjunto con Oxford Economics, muestra que el sector de viajes y turismo experimentó un crecimiento del 3,5% en 2019, superando el crecimiento de la economía mundial del 2,5% por noveno año consecutivo. En los últimos cinco años, el sector creó uno de cada cuatro nuevos puestos de trabajo, lo que convierte a Viajes y Turismo en el mejor elemento para que los gobiernos generen empleo.
Según informe de OMT del Turismo Mundial, el 2019 ha sido el décimo año consecutivo de crecimiento del turismo.
La región de Oriente Medio ha sido la región con un mayor crecimiento en cuanto a las llegadas de turistas internacionales en 2019, habiendo duplicado casi la media mundial (+8%). El crecimiento en Asia y el Pacífico se ralentizó, pero sigue arrojando un crecimiento superior a la media, con un aumento del 5% en el número de llegadas internacionales. Europa, donde el crecimiento fue también inferior al de los años previos (+4%) sigue a la cabeza en términos de número de llegadas internacionales, con 743 millones de turistas internacionales el pasado año (el 51% del mercado mundial). Las Américas (+2%) ofrecieron unos resultados heterogéneos, ya que si bien muchas islas caribeñas consolidaron su recuperación tras los huracanes de 2017, al mismo tiempo el número de llegadas a Sudamérica cayó, debido en parte a los disturbios sociales y políticos. Para África (+4%) se dispone de datos limitados, pero se observa el mantenimiento de unos resultados muy positivos en el Norte de África (+9%) y un menor crecimiento en el África Subsahariana (+1,5%). Podemos observarlo en la tabla siguiente:

Tabla 20.- Crecimiento del turismo a nivel mundial



Así pues, en 2019 se registraron 1.500 millones de llegadas de turistas internacionales en el mundo.
Se esperaba que este incremento del 4% con respecto al año anterior se repitiera en el 2020, pero la crisis mundial provocada por la pandemia, ha cambiado mucho las expectativas y ha aumentado las incertidumbres.

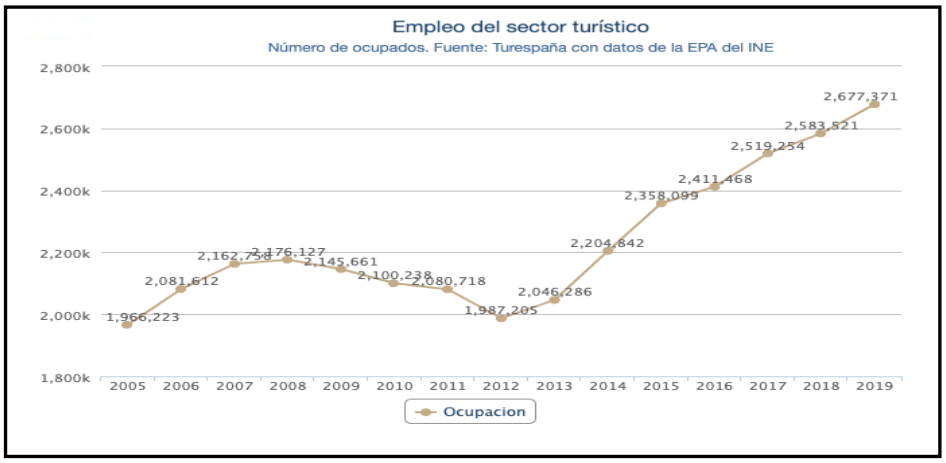
3.2. El sector turístico en la economía europea

El turismo europeo realiza una contribución al PIB mundial de 2 billones y una contribución al empleo mundial de 37,1 millones, cifras suficientemente contundentes como para considerar el sector turístico, un sector muy importante y con marcado carácter emergente.
Siguiendo con los estudios del WTTC, Europa sigue siendo la región más grande del mundo en términos de gasto de visitantes internacionales (US $ 619 mil millones) y representa el 37% de todo el gasto internacional global en 2019. Además, es significativo el hecho que mientras que la economía europea creció solo un 1,3%, el sector de Viajes y Turismo mostró un mayor crecimiento, el 2,4%.
Destacar que las mayores economías europeas en términos de viajes y la contribución del turismo al PIB en 2019, fueron Alemania (US $ 347 mil millones), Italia (US $ 260 mil millones), Reino Unido (US $ 254 mil millones) Francia (229 mil millones de dólares) y España (198 mil millones de dólares).
Entre todas las economías europeas, Grecia fue la que tuvo un crecimiento más rápido con un 12,1% en 2019, casi seis veces mayor que el crecimiento económico general. También, tuvo un fuerte crecimiento Turquía, gracias sobre todo a las mejoras de seguridad, entre otras razones. Y Portugal, donde los viajes y el turismo representaron 16,5% de la economía total, el PIB del sector creció en 4.2%.
Los crecimientos en el sector turístico suponen siempre iniciativas para superar la estacionalidad.

Con todo ello, y centrándonos ya en España podemos decir que el nuestro, es el primer país de Europa y el tercero en todo el mundo en gasto de visitantes internacionales (US $ 86,8 mil millones).
Además indicaremos que el sector turístico representa un 14,3% del PIB total del estado Español, con una tendencia ascendente del 1,8% durante el año 2019

En segundo lugar, nos centraremos en el empleo que genera el sector. Los datos son muy elocuentes, se generaron un total de 2.677.371 de puestos de trabajo en 2019 lo cual representa un 13,4% del empleo total del país. También cabe destacar que la tasa de paro del sector (12,1%) fue inferior a la media nacional (13,8%) y que durante el último trimestre del año pasado mejoró la calidad del empleo originado por el sector, produciéndose un aumento del 10,2% de los contratos indefinidos frente a un decremento del 3,2% de la contratación temporal.

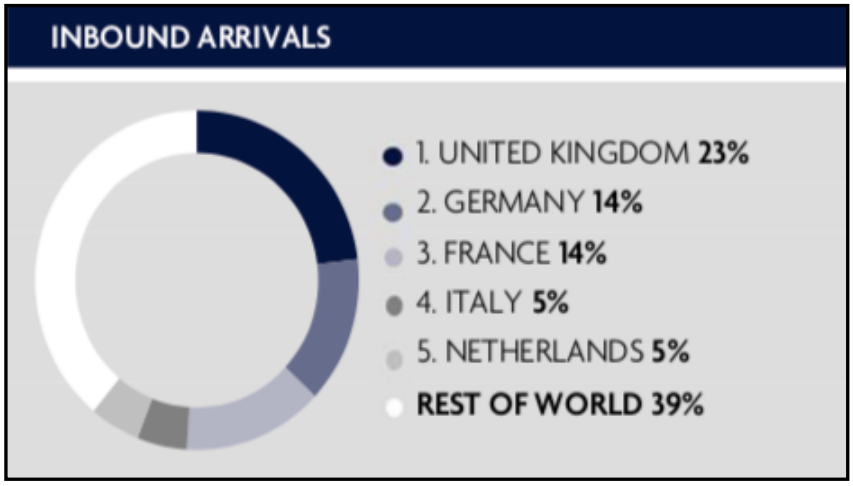
Tabla 21.- Evolución de la ocupación en España en el sector turístico



Analizando los datos vemos que el incremento de la ocupación en el sector turístico iba en ascenso desde 2005 a 2010, cuando empieza a tener un significativo descenso en la crisis de 2012. A partir de ahí la recuperación en el sector ha ido en ascenso hasta colocarse en niveles de ocupación tan altos que pueden considerarse como máximos históricos hasta el 2019. Los datos finales del 2019 sufrirán una alteración significativa en el sector debido a la pandemia que estamos padeciendo, que ha alterado todo el sistema productivo y en especial al sector turístico.

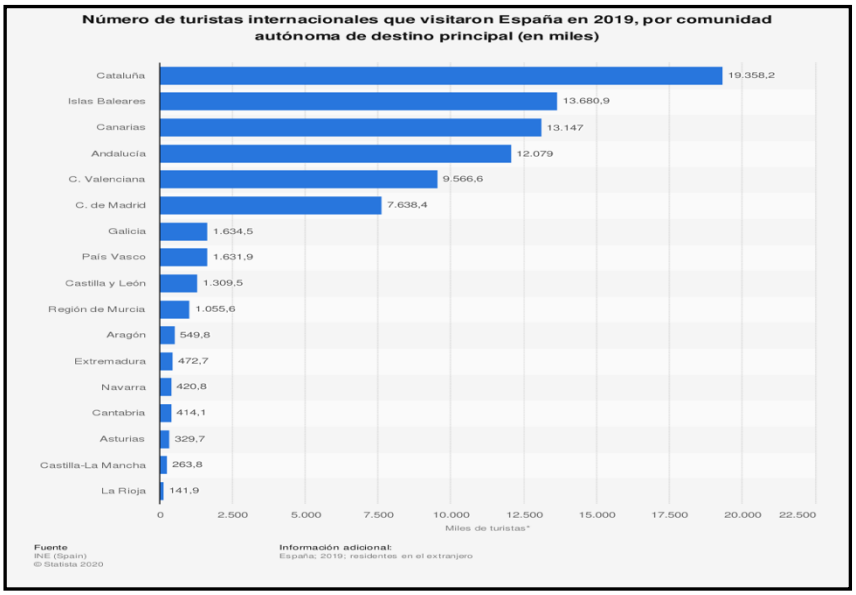
En tercer lugar, nos parece fundamental realizar una breve observación respecto a la nacionalidad de los turistas que llegan a España. Podemos ver la distribución en el siguiente gráfico ofrecido por el World Travel & Tourism Council en el año 2019.
En el gráfico adjunto se observa claramente que nuestro turismo es mayoritariamente europeo, destacando el turismo proveniente de Reino Unido- ingleses, seguido de alemanes y franceses en los puestos más destacados. La diferencia con el resto de nacionalidades es claramente significativa.

Gráfico 22.- Turistas que llegan a España por nacionalidades



En cuarto lugar, nos parece significativo visualizar, cuáles son las comunidades autónomas a las que se dirigen de forma prioritaria los turistas internacionales durante el año 2019. Como se puede observar en el gráfico que exponemos a continuación, las comunidades que más turistas internacionales reciben son: Cataluña, claramente diferenciada con el resto, le siguen Baleares, Canarias y Andalucía y en tercer lugar podríamos situar a las comunidades Valenciana y Madrid, ya con una significativa diferencia del resto.

Tabla 23.-Comunidades autónomas de destino del turista internacional



Finalmente, nos parece interesante señalar que el turismo de ocio representa un 89% frente a un 11% del turismo ligado al trabajo, lo cual es acorde al sistema de turismo que solemos ver basado en la atracción del clima, la costa y las tradiciones del país.

Como conclusión tras el análisis de todos los datos expuestos podemos afirmar que el sector turístico español hasta el año 2019 ha sido uno de los sectores más importantes para la economía española con un elevado valor del PIB y además en tendencia alcista. Además genera altos niveles de ocupación y con tendencia a contrataciones indefinidas. Ambos factores hacen que el sector turístico, tenga un alto potencial para la economía.
Y respecto al perfil del turista que nos visita podemos concluir que es fundamentalmente europeo: ingleses, alemanes y franceses, sobre todo y que se dirigen a comunidades como Cataluña, Baleares, Canarias, Andalucía, Comunidad Valenciana y Madrid, buscando un turismo de ocio.

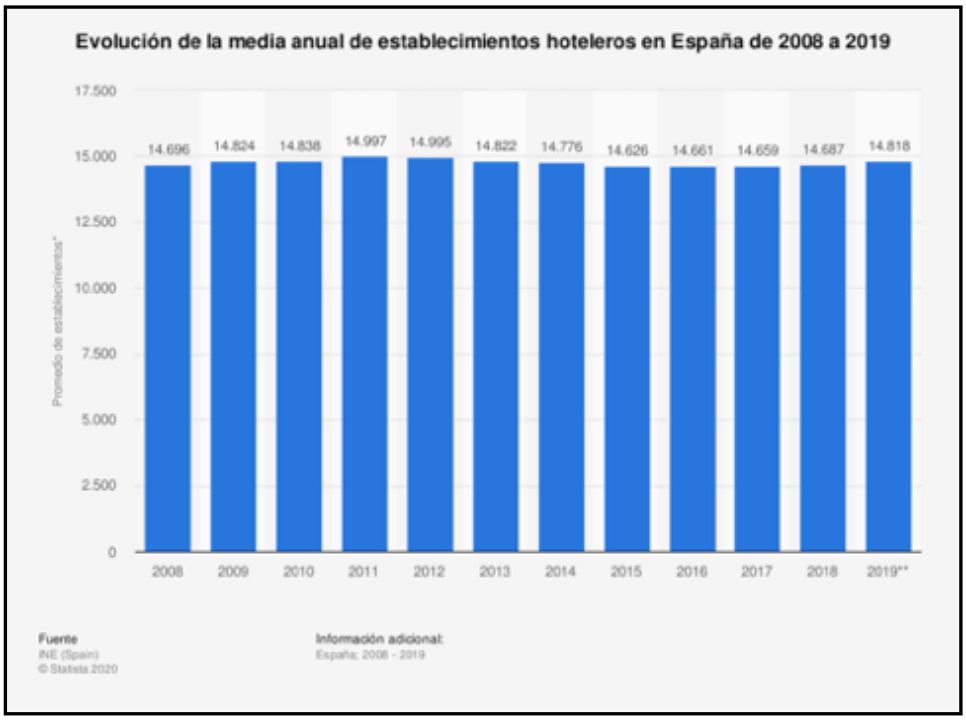
3.3. Importancia de los hoteles en el sector turístico

Habiendo comentado anteriormente que aproximadamente, el 14,3% del PIB español es debido al sector turístico, vamos a centrarnos concretamente en el sector hotelero que es uno de los mayores activos del turismo español.

Para estudiar la importancia de los hoteles en el sector turístico vamos a analizar: el número de establecimientos hosteleros, los ingresos o rentabilidad que suponen y el número de turistas extranjeros, que hemos visto que son mayoritarios, alojados en establecimientos hosteleros comparados con los no hoteleros.

Si analizamos la tabla siguiente, observaremos la evolución del sector hostelero a lo largo de los últimos 10 años.

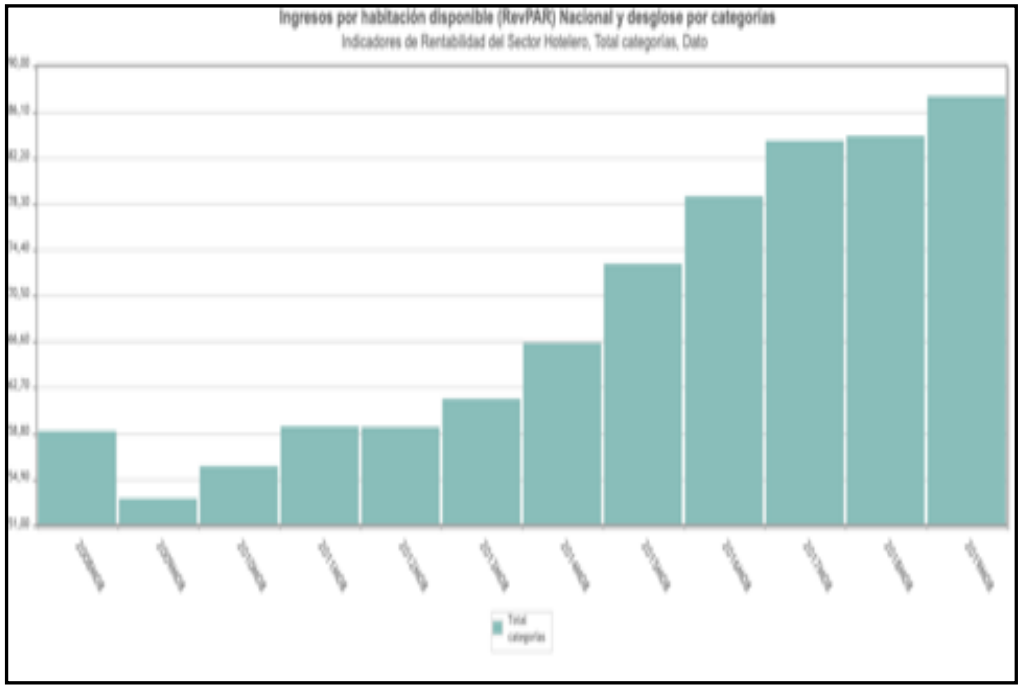
Tabla 24.- Evolución de los establecimientos hosteleros



En el gráfico, observamos que la evolución del sector en cuanto al número de establecimientos hosteleros permanece bastante estable con el paso de los años, solamente con un ligero pico en el año 2011 que permanece en el año siguiente. A partir de ahí hay ligeros descensos continuados hasta el 2018, que tiende al alza en el 2019.

Para analizar la evolución de la rentabilidad del sector utilizaremos el indicador RevPar (Revenue Per Available Room). Este indicador se calcula dividiendo los ingresos por habitación entre las habitaciones disponibles y otorga una visión general bastante cercana a la realidad.

Tabla 25.- Indicador RevPar



Como se puede ver se ha seleccionado el mes de mayor ocupación (agosto) de los últimos diez años para poder comparar la evolución.
Observamos que excepto en 2009 a causa de la crisis económica la evolución ha sido positiva situándose en 2019 el ingreso medio por habitación disponible en 87,32 según el INE.

Tras el análisis de la evolución del sector en cuanto a establecimientos e ingresos procedemos a comparar la ocupación del sector en establecimientos hoteleros y los alojamientos en establecimientos no hoteleros durante los últimos 20 años.

Tabla 26.- Turistas extranjeros alojados en establecimientos hoteleros

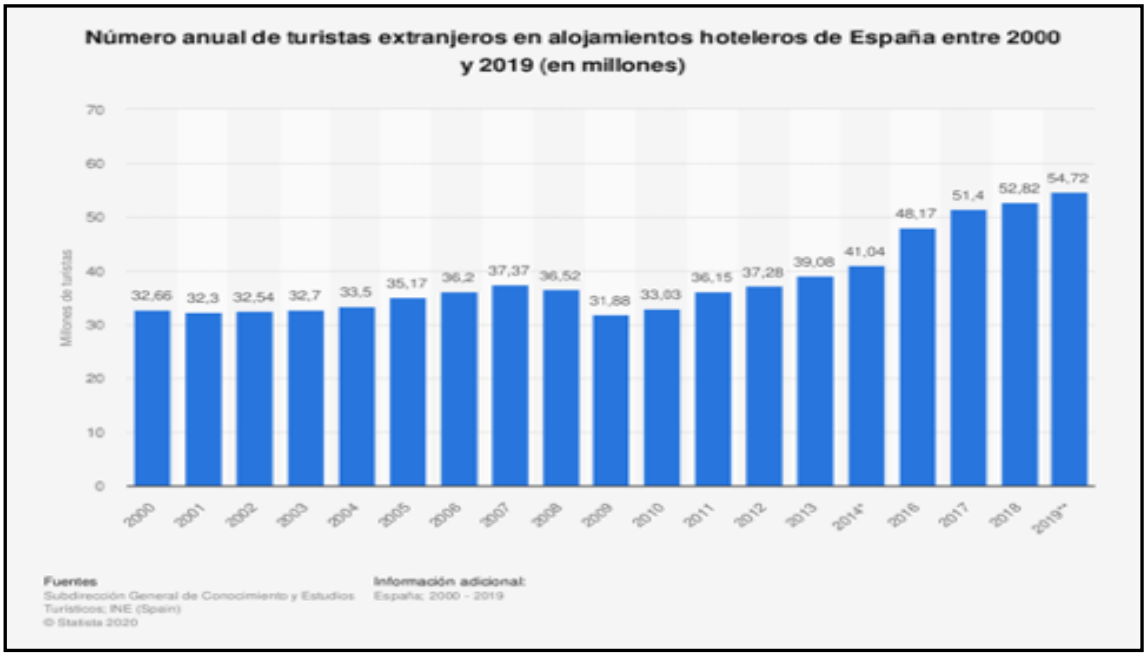
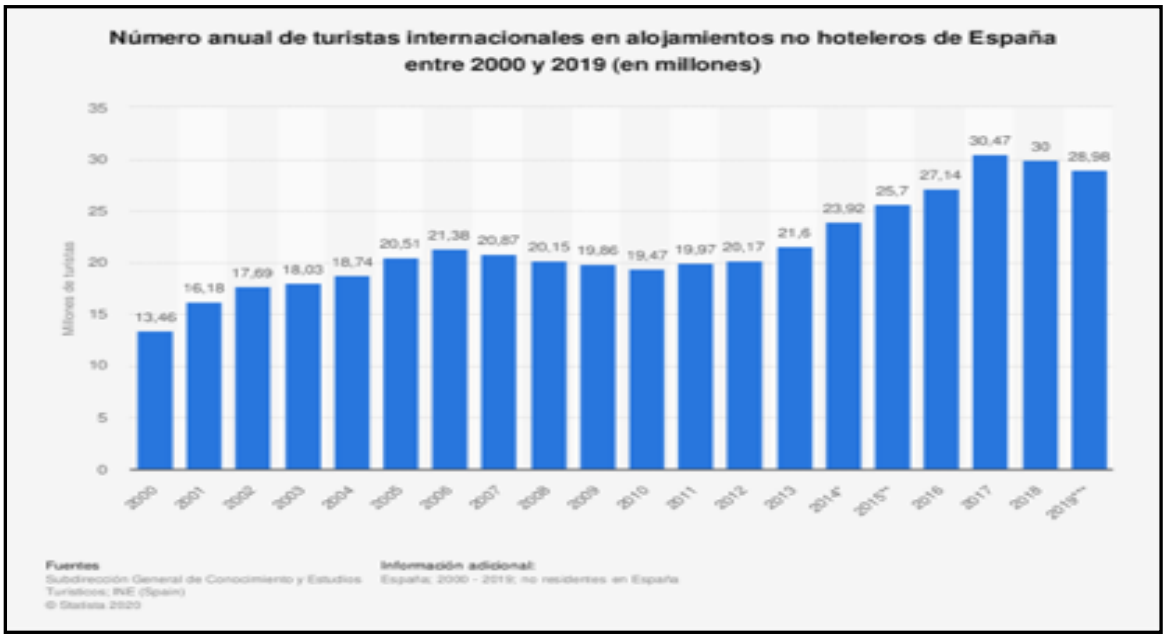


Tabla 27.- Turistas extranjeros alojados en establecimientos no hoteleros



Como observamos en la primera tabla, entre los años 2000 y 2013 el alojamiento de los turistas extranjeros en establecimientos hoteleros, se sitúa siempre en valores entre el 30 y el 39% con sensibles variaciones. Pero, es a partir del 2014 cuando se supera el 40% llegando a situarse en el 54% en el año 2019, siendo el porcentaje más alto registrado.

Si analizamos ahora, la segunda tabla, comprobaremos los porcentajes de turistas internacionales que prefieren alojarse en establecimientos no hosteleros. En los primeros años y de forma progresiva se llega alrededor del 20% en el 2005 que se mantiene con ligeros descensos hasta el 2012. A partir de este momento empieza a ascender llegando a más del 30% en el 2018, porcentaje más alto registrado, volviendo a descender con valores debajo del 30%, en el 2019.

Así pues podemos concluir que el número de establecimientos hosteleros se mantiene estable a lo largo de los últimos años, que el ingreso medio por habitación disponible(según nos indica el REvPar) ha ido evolucionando positivamente y que los turistas extranjeros prefieren alojarse en establecimientos hosteleros frente a los no hosteleros. Por todo ello, consideramos bien fundamentado la elección del sector hostelero como objeto de estudio.

3.4. Categorización de hoteles

En la actualidad no existe ningún criterio de categorización de los hoteles de forma homogénea en Europa ni siquiera en España, aquí la competencia reside en cada comunidad autónoma aunque en la realidad los criterios son bastante uniformes ya que las diferencias entre comunidades son mínimas.
Según la Confederación Española de Hoteles y Alojamientos Turísticos (CEHAT) es obligatorio solicitar la clasificación del establecimiento hotelero que se mantendrá mientras se cumplan los requisitos. Estos son los requisitos mínimos por categoría y comparándolas entre sí:

- 1 Estrella: Habitación doble de 12 metros cuadrados mínimo, habitación individual de 7 metros cuadrados mínimo, cuarto de baño (baño o ducha) de 3,5 metros cuadrados mínimo, calefacción y ascensor.
- 2 Estrellas: Las variaciones respecto a una 1 estrella, son que los metros cuadrados de la habitación aumentan a 14, teléfono en habitación y servicio de caja de seguridad

- 3 Estrellas: Aumentan respecto a los de 2 estrellas, los metros cuadrados de las habitaciones dobles, individual y cuarto de baño que pasan a 15, 8 y 4 respectivamente. Además incluyen aire acondicionado en zonas comunes y bar.
- 4 Estrellas: Añaden a los de 3 estrellas, mayor metros cuadrados en los espacios anteriormente indicados que pasan a ser, 16, 9 y 4,5 respectivamente. Y añaden aire acondicionado en habitación y caja fuerte.
- Y en el 5 Estrellas: Los metros cuadrados de los espacios descritos son 17, 10 y 5, respectivamente. El resto de servicios mínimos ya son igual que en los de 4 estrellas.

Pero consideramos que debemos dar una mayor profundidad al tema, por ello y como ejemplo se ha decidido tomar la tabla clasificatoria de los criterios de Andalucía (que adjuntamos a continuación) la cual se puede extrapolar a cualquier comunidad autónoma. Es de destacar que la clasificación va en función de los servicios ofrecidos no en función de la calidad de estos.

Tabla 28.- Criterios de clasificación de hoteles (Andalucía)

Nº DE ESTRELLAS	5	4	3	2	1
ZONA DE COMUNICACIONES					
Accesos diferenciados para usuarios y personal de servicio	SI	SI	SI	NO	NO
Guardarropas en el vestíbulo	SI	NO	NO	NO	NO
Ascensores (nº ascensores/nº de plantas)	2/2	1/2	1/2	1/3	1/3
Pasillos (anchura mínima en m)	1,75	1,6	1,5	1,3	1,2
Escaleras (anchura mínima en m)	1,5	1,4	1,3	1,2	1,2
ZONA DE USUARIOS					
Suites	5%	NO	NO	NO	NO
Suites Junior	SI	SI	NO	NO	NO
Baños	**Completo** (ducha, bañera, dos lavabos, bidé e inodoro)	El **50%** de las habitaciones dispondran de **baño completo**		El **25%** de las habitaciones dispondran de **baño completo**	Solo es obligatorio **aseo**
GARAJE	Si el garaje o aparcamiento se ubica en otro edificio concertado, los hoteles de cinco estrellas contarán con personal para prestar el servicio de aparcamiento				
CLIMATIZACIÓN					
En **habitaciones,** con mando independiente	SI	SI	NO	NO	NO
En **zonas comunes**	SI	SI	SI	NO	NO
COMUNICACIONES					
Teléfono en baño	SI	NO	NO	NO	NO
Teléfono en oficios por planta	SI	SI	SI	NO	NO
Internet	SI	SI	NO	NO	NO
SERVICIOS					
De **equipaje**	SI	SI	NO	NO	NO
De **habitaciones**	24 horas	SI	SI	NO	NO
De **bar**	SI	SI	SI	NO	NO
De **comedor**	SI	SI	SI	NO	NO
De **lavanderia**	SI	SI	SI	SI	NO
Sanitarios (botiquin y médico)	SI	SI	SI	SI (más de 40 habitaciones)	
Seguridad	Caja fuerte en la habitación		-	-	
Mantenimiento	24 horas al dia		-	-	

Como podemos observar los criterios de clasificación se dividen en los siguientes apartados: zona de comunicaciones, zona de usuarios, garaje, climatización, comunicaciones y servicios. Según se disponga del servicio o no, los metros de los espacios o el número de elementos, se asigna el número de estrellas.

En la zona de comunicaciones, se tienen en cuenta: accesos, ascensores, pasillos, escaleras y guardarropas. En la zona de usuarios, se tiene en cuenta los tipos de habitaciones y sus dimensiones, así como los baños. Para la zona de aparcamiento o garaje, se tiene en cuenta si está en el mismo edificio o fuera o incluso si puede tener aparcacoches. En la climatización se distingue la de las habitaciones y su nivel de dependencia ,de las zonas comunes. Respecto a las comunicaciones, se tienen en cuenta los servicios de teléfono e internet. Y por último, por su gran amplitud de elementos, destacan los servicios que se clasifican en: equipaje, habitaciones, bar, comedor, lavandería, sanitarios, seguridad y mantenimiento.

Pero avanzando en el nivel de unificación de criterios y en el plano europeo, bajo el patronato de HOTREC (Confederación Europea de Hoteles y Restaurantes) nació en 2009 Hotelstars Union con 7 países adscritos: Austria, Alemania, Suiza, República Checa, Hungría, Holanda y Suecia con el fin de crear unos criterios unificados para toda Europa. Con el paso del tiempo se han ido sumando más países, hasta alcanzar los 17, principalmente del centro y norte de Europa. En la actualidad, España está negociando su incorporación, con la intención de ser el primer país del sur de Europa en formar parte de Hotelstars Union.
Hotelstars Union posee un criterio unificado. Había uno establecido hasta 2020, pero para afrontar los nuevos retos del sector se ha actualizado. Éste entrará en vigor a partir del 1 de enero de 2021.
A continuación, se van analizar los puntos del nuevo criterio de Hotelstars más relacionados con el objeto de este trabajo.
En el anexo 1 de este trabajo, se detallan todos los criterios agrupados por áreas de Hotelstars Union valorados mediante un sistema de puntos y requisitos básicos de cada categoría.
Hay diferentes apartados en los que se detalla desde el tamaño de la habitación y la cama hasta unas directrices básicas de cómo debe de ser la web del hotel.

Haciendo hincapié en el objeto del trabajo se puede ver que ni siquiera en los hoteles de 5 estrellas hay un requerimiento de una conexión segura para los clientes mediante una VPN o una LAN segura.

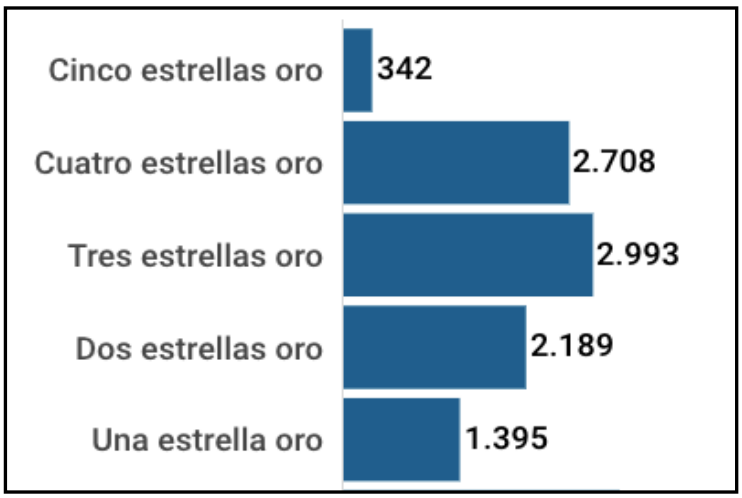
A parte de los hoteles los cuales hemos estudiado su categorización anteriormente, dentro del sector de alojamientos hoteleros también encontramos los hostales, pensiones, moteles y los hoteles-apartamentos sobre los cuales solo se van tratar las diferencias de forma muy breve ya que no son el objetivo del trabajo.
En el caso de los hostales, no cumplen los requisitos para ser considerados hoteles y se ubican en uno o varios pisos correlativos y comunicados entre sí por escalera interna de uso exclusivo, dentro de un mismo edificio. Deben tener un mínimo de 10 habitaciones y 20 plazas y pueden ser de 1, 2 o 3 estrellas.
Las pensiones, no cumplen los requisitos para ser considerados hoteles ni hostales. Pueden tener o no comedor, y en caso de que lo tengan, pueden ofrecer solo tarifas de pensión completa. De la misma forma que los hostales pueden ser de 1 a 3 estrellas.
Los moteles**,** se consideran como tales los hoteles situados a menos de 500 metros del eje de la carretera, con entrada independiente y garaje o aparcamiento cubierto para tantos coches como habitaciones tenga.
Y finalmente los hoteles-apartamentos, además de las características de un hotel, disponen de cocina y espacio para comer dentro de cada habitación. Deben disponer de cocina, salón, uno o varios dormitorios y cuarto de baño. Al igual que los hoteles, los apartahoteles también se valoran entre 1 y 5 estrellas, en función principalmente a las medidas de sus habitaciones

Así pues hablar de categorización de los hoteles, es hablar del número de estrellas que se les asigna en función de las instalaciones y de los servicios disponibles y aunque se tienden cada vez más a una unificación de criterios, la realidad es que no existen una homogenización de criterios, aunque cada vez más se tiende a ello. Parece ser que Hotelstars es una buena solución y por ello, España está intentando adherirse a dicha asociación.

3.5. Propuesta de Pyme en el sector hotelero

Los datos aportados por el INE en junio de 2019, nos indican el número de establecimientos hoteleros según el número de estrellas. Se puede observar que los de 3 estrellas son los más numerosos, seguidos de los de 4 estrellas y de los de 2 estrellas. En los extremos por arriba se encuentran los de una estrella y los menos numerosos de forma significativa son los de cinco estrellas.

Tabla 29.- Clasificación de número de hoteles por estrellas



Fuente: INE, datos correspondientes julio 2019

Tras observar los datos anteriores, sobre el la cantidad de hoteles en España por categorías hemos comprobado que el tipo de hotel más común es el de "*3 estrellas*", con 2993 establecimientos a lo largo de la geografía nacional. Por ello vamos a usar esta categoría para elaborar un modelo de Pyme hotelera que sirva para posteriormente elaborar un plan de seguridad en base a los riesgos y recomendaciones que se verán más adelante.

Siguiendo el Criterio de mínimos de hotelstars union, el hotel de 3 estrellas, propuesto cuenta con un sitio web bilingüe con información actualizada, incluyendo el tamaño de las camas, imágenes realistas y la ubicación del hotel, acceso a internet mediante WiFi en las zonas comunes y en las habitaciones y una estación de carga de dispositivos con diferentes adaptadores bajo demanda.

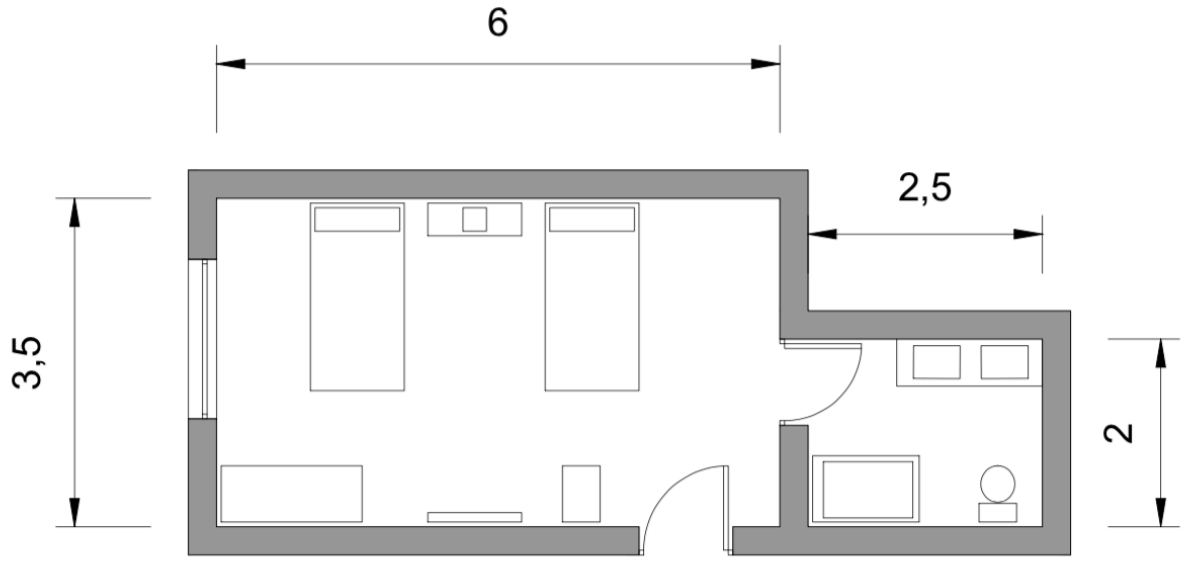
Además de estos requisitos mínimos, en dicho hotel también se ofertan los siguientes servicios tecnológicos:

- App del hotel con información y servicio de llave digital.
- Televisor Smart Tv en cada habitación

Además el futuro en los hoteles aplica las mismas soluciones que en las viviendas. Por eso, la domótica puede llegar a ser una parte esencial del servicio hotelero. Los usos más comunes son la climatización y la iluminación. La domótica favorece y facilita las tareas de mantenimiento, así como un ahorro considerable de cantidad de energía eléctrica. Pero la realidad es que la domótica en los hoteles, al igual que en las casas, aún no se ha generalizado, por ello, a nuestra habitación, además de los elementos ya enumerados, añadimos:

- Domótica básica en cada habitación: persianas y luces

Tabla 30.- Habitación propuesta



4. SERVICIOS DE TECNOLOGÍA MÁS FRECUENTES EN EL SECTOR HOTELERO ESPAÑOL

Llegados a este punto del trabajo, queremos empezar indicando el nivel de informatización de las PYMES españolas que se expuso en el punto 2.3, en el que se comparaban los distintos sectores productivos y en el que respecto al sector "hoteles y agencias de viajes" concluimos que:
1.- Los hoteles son entornos con buenas dotaciones de ordenadores y con una alta accesibilidad a internet, en el caso de nuestras PYMES
2.- La presencia y uso de internet en los hoteles y agencias de viajes, podemos decir que está prácticamente implantado en la mayoría de los mismos. Además que tienen una alta disponibilidad de páginas web y que su presencia a través de medios sociales está consolidada.
3.- Las ventas realizadas a través de internet es uno de los puntos fuertes del sector hoteles y agencias de viajes.
4.- Escaso uso de herramientas de cloud computing y que el uso de herramientas de ciberseguridad en este caso está desarrollado si se compara con otros sectores.
5.- La presencia de especialistas TIC y la formación en este campo, es una de las tareas menos desarrolladas en este sector.

Así pues, podemos indicar que la informatización del sector hotelero no es de las más desarrolladas pero podemos asegurar que se encuentra en un punto intermedio alto, respecto a los otros sectores.

En segundo lugar, y partiendo del trabajo de Eugenia Cámpora Espí sobre el "Estudio del impacto de las TIC en el turismo: análisis de su influencia en los habitantes de la ciudad de Gandía durante la planificación de un viaje" y en concreto en el apartado "Impacto de las TIC en los hoteles" podemos añadir que:
1.- El impacto de internet en los establecimientos hoteleros, está relacionado principalmente con el concepto de comercialización.
2.- Las TIC en el ámbito hotelero ha impactado también, y de forma muy significativa en la gestión interna de los hoteles.
Internet es probablemente una de las TIC que más ha revolucionado el sector hotelero, y ha ido modificando poco a poco la manera en que éste opera. Ha ofrecido ventajas a los hoteles como: difusión de una gran cantidad de información, mayor participación por parte del cliente, interconexión de servicios, mejora de la calidad del servicio prestado al cliente, acceso a la información las 24 h del día y 7 días a la semana y reducción de costes en intermediarios al poder distribuir sus productos directamente al cliente a través de la página web.
Y dentro del acceso que proporciona internet y vinculado con la gestión hotelera, dentro de la web destacan: los blogs y las redes sociales por todo aquello de la información que recogen de los clientes para adaptar cada vez más y mejor el servicio al cliente.
Y respecto a los nuevos canales de distribución, destacan las páginas web y su gestión de reserva on line.
Uno de los avances más significativos del sector.

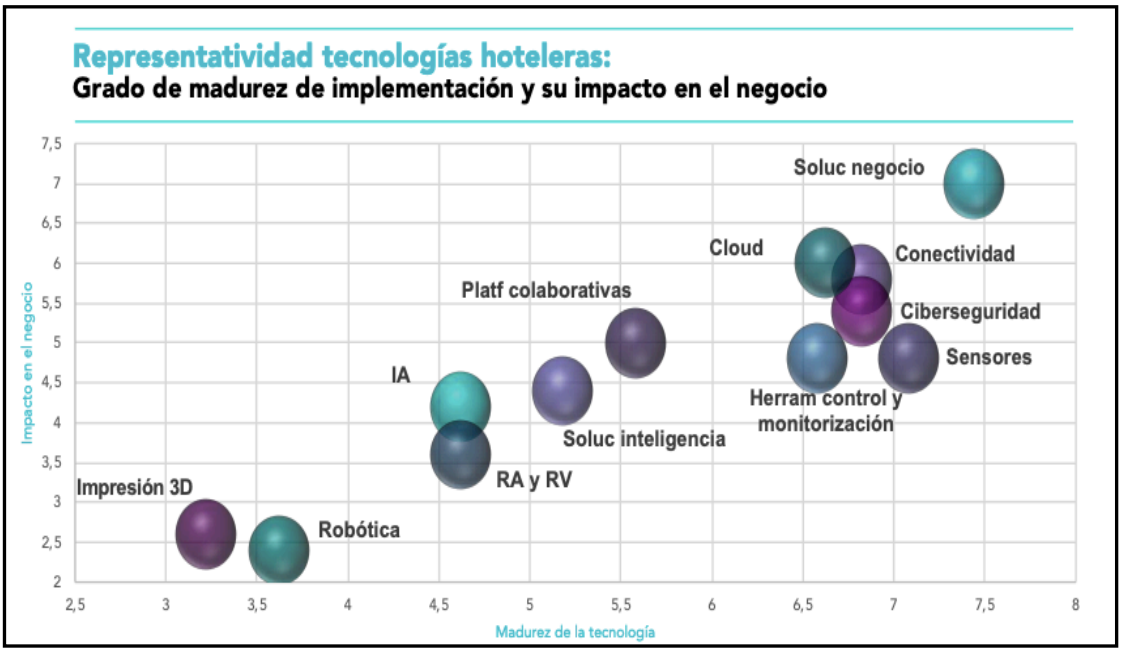
Además resulta especialmente interesante las aportaciones de la autora, en cita de Miralles (2008), las herramientas o aplicaciones informáticas que más se utilizan en los hoteles:
1.- Property Management Systems (PMS). Es un sistema de información básico para la gestión hostelera
2.- Customer Relationship Management (CRM). Es un sistema de gestión de las relaciones con los clientes.

Así pues, de sus aportaciones concluimos que internet ha revolucionado la comercialización y la gestión de los hoteles, quienes a través de sus web y canales de distribución han facilitado mucho el acceso a la información del cliente y por lo tanto, la distribución y disponibilidad de sus establecimientos hoteleros. Además ha facilitado mucho la gestión hotelera con programas específicos tanto para facilitar las relaciones con los clientes, como para en general, mejorar la gestión hostelera.

A continuación, queremos centrar el punto y la atención, en el estudio sobre PERCEPCIÓN Y USO DE LA TECNOLOGÍA POR EL CLIENTE 4.0 EN EL SECTOR HOTELERO del Instituto Tecnológico Hotelero (ITH).
En él se afirma que, el 70,6% de los huéspedes hacen un uso muy alto de la tecnología en su día a día y 1 de cada 3 afirma que la tecnología ofrecida por el alojamiento hotelero es un aspecto decisivo a la hora de elegir un establecimiento.

Por esto no es de extrañar que los hoteles inviertan cada vez más en las nuevas tecnologías con el fin de satisfacer estas nuevas necesidades de sus clientes.
En el siguiente gráfico podemos ver la relación entre la madurez de distintas tecnologías y el impacto en el sector:

Tabla 31.-Madurez de la tecnología e impacto en el negocio hotelero



Se observa que la impresión 3D y la Robótica son las tecnologías menos maduras en el sector. En cambio, la solución del negocio es la más madura. En niveles intermedios se encuentran las plataformas colaborativas y la ciberseguridad, a pesar de ser una tecnología bastante madura, está un poco por debajo del impacto esperado siguiendo con la tendencia del gráfico.

Y para finalizar y entrando en materia sobre los servicios tecnológicos a desarrollar en el sector, definimos las etapas y definiciones propuestas por el ITH: Inspirar, Planificar, Contratar, Estancia y Compartir y que especificamos a continuación:

La primera etapa, INSPIRAR, hace referencia al momento en el que los clientes tiene la necesidad de buscar un alojamiento para su viaje. El servicio que puede ofrecer el hotel en este caso es la presencia en buscadores y redes sociales.

En segundo lugar, PLANIFICAR donde los clientes tienen acceso a distintas opciones de alojamiento, comparan e interactúan para tener clara su decisión. Para poder ser la opción elegida por el cliente el hotel puede aparecer en compradores y/u ofrecer una web propia que puede tener un chat directo e incluso un tour por el hotel en realidad virtual.

La tercera etapa, es CONTRATAR, momento en el que los clientes efectúan la reserva a través de los distintos medios que les ofrecen, según el ITH los más extendidos son los compradores y la propia web del hotel y en el caso de clientes fidelizados WhatsApp o algún servicio de mensajería instantánea similar.

La siguiente etapa es la ESTANCIA, etapa en la que el cliente hace su llegada al hotel, se instala y tiene diversas tecnologías a su alcance, estas son: Check-in virtual, puestos de carga móvil, llaves digitales, domótica, chromecast/smart TV, WIFI, MIFI, Impresora 3D, Handy Phone, Gafas de Realidad Virtual, Apps hotel, oferta complementaria de servicios, Patinetes eléctricos, comunicación directa con el hotel mediante apps de mensajería instantánea (Whatsapp), reconocimiento facial emociones, Tablet, Sistema Alerta sonidos, Check-out virtual…

Finalmente, la quinta y última etapa es la COMPARTIR, etapa en la que los clientes transmiten su experiencia tanto a otros clientes como a los hoteles tras su alojamiento, a través de distintos canales y herramientas tecnológicas como las redes sociales, la web del hotel, portales de reserva o internamente mediante encuestas

Así pues, teniendo en cuenta estas etapas por las que pasa el cliente, es el establecimiento hostelero quien debe planificar tendiéndolas en cuenta y adecuando los servicios tecnológicos más adecuados para dar la mejor respuesta posible al cliente.

Y tener en cuenta la importancia que se da a la tecnología según el tipo de viajero tal y como se expone en la tabla adjunta.

Tabla 32.- Importancia de la tecnología según tipo de viajero

Cantidad de viajeros que consideran muy importante la tecnología a la hora de hospedarse.

*Consideramos como muy importante aquellos que valoran 8-10 en la pregunta de importancia tecnológica.

Tipo viajero	Importancia tecnología
Aventurero	53,4%
Urbanita	49,2%
Vacacional	48,5%
Cultural	40,6%
Gastronómico	39,8%
De negocios	39,3%
De interior	12,9%

Los distintos perfiles de viajero, salvo el de interior, dan mucha importancia a la tecnología a la hora de elegir un alojamiento, pero no tienen expectativas muy altas respecto a la innovación tecnológica disponible cuando viajan. Hospedarse en lugares que ofrezcan una tecnología innovadora les provoca sorpresa generando mayor vinculación y niveles más altos de recomendación.

Viajeros aventureros, urbanitas y vacacionales, los turistas que más valoran la tecnología en los alojamientos.

Más de la mitad de viajeros aventureros le dan una importancia muy alta a la tecnología. Este perfil, en términos generales es innovador y tiene conocimiento de los últimos avances en tecnología.

En ella podemos observar, que el perfil del viajero que más valora la tecnología en los hoteles son los aventureros, los urbanitas y los vacacionales. Lo que más llama la atención es que precisamente el hombre de negocios que parece tenga que depender más de las nuevas tecnologías, se encuentra en los últimos lugares de la valoración. Por contra parece normal que sean los de interior los que menos valoren este servicio, frente a los urbanitas que se encuentran en los primeros lugares, pensamos que está más vinculado a la dependencia que genera la facilidad de acceso como es en las ciudades frente a las dificultades que aún pueden tener en algunos sitios del interior. Y el hecho que los aventureros y viajeros se encuentren en los primeros lugares, demuestra la importancia que las nuevas tecnologías tienen para los viajes, de ahí que los hoteles para atender mejor a los clientes, deben estar bien dotados tecnológicamente.

5.- IDENTIFICACIÓN DE RIESGOS INFORMÁTICOS Y RECOMENDACIONES DE SEGURIDAD

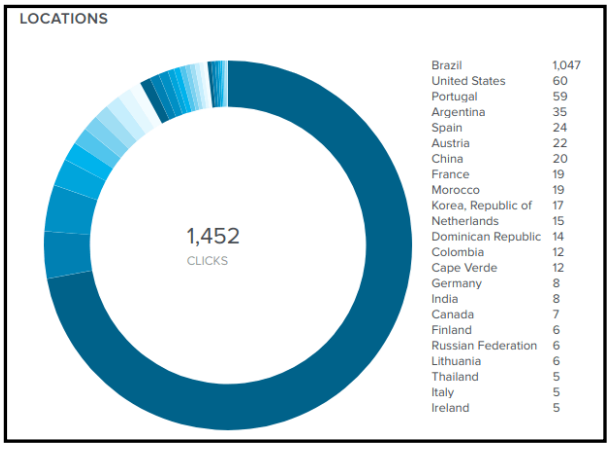
En el punto anterior hemos revisado brevemente los servicios de tecnología más frecuentes en los establecimientos hoteleros españoles, llegando a la conclusión parcial que las tecnologías en todas sus dimensiones no solo son importantes sino que son condicionantes para el cliente y para el establecimiento hotelero. Pero llegados a este punto, vamos a analizar los niveles de seguridad de los servicios tecnológicos según categorías de hoteles. Para ello, primero revisaremos los ataques conocidos más frecuentes, a continuación identificaremos algunos de los riesgos más significativos, para finalmente recomendar la seguridad necesaria, siguiendo el modelo ISO270012.

5.1. Ataques más frecuentes: casos conocidos más recientes

Vistas pues, las tecnologías ofrecidas con más asiduidad por los establecimientos hoteleros, a continuación se va a realizar una recopilación de los ataques más frecuentes que se han producido en la actualidad. Cada ataque está asociado a un suceso real de compañías del sector que los han sufrido, para así poder medir con mayor precisión, el alcance del problema que supone la afección de un ataque informático.

En primer lugar, tenemos el "*spear phishing*" que según Kaspersky es una estafa de correo electrónico o comunicaciones electrónicas dirigida hacia un individuo, una organización o un negocio determinados. Aunque a menudo está destinada a robar datos con fines maliciosos, los cibercriminales también pueden intentar instalar malware en el ordenador de un usuario específico.
Relacionado con este ataque encontramos el caso de RevengeHotels, una campaña de cibercrimen focalizada en hoteles, estuvo activa desde 2015 hasta 2019 y se dedicó a robar y vender información sensible de clientes, principalmente crediticia, y también permitió, accesos directos a máquinas de administración de dichos hoteles a otros delincuentes.
Principalmente afectó a hoteles de Brasil, pero se extendió a 22 países más, entre ellos España, existiendo constancia de que afectó al menos a 1452 pudiendo ser muchos más, de los cuales no se ha obtenido información. El siguiente gráfico ofrecido por la empresa bit.ly tras el análisis de un enlace acortado malicioso usado por los cibercriminales detalla los posibles casos en los países afectados.

Tabla 33.- Posibles casos en los países afectados por "*revenghotels*"



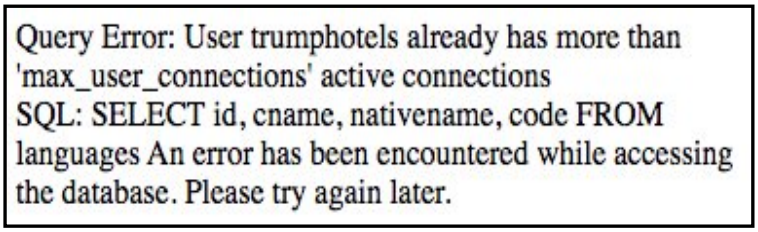
Como se puede observar y ya hemos indicado, se produjo principalmente en Brasil, pero afectó también, aunque con muchos casos menos detectados y en este orden a Estados Unidos, Portugal, Argentina y España.
Actualmente, se siguen investigando casos de phishing parecidos que podrían pertenecer a la misma campaña de phishing que hemos analizado. Para intentar minimizar estos efectos, se recomienda a los huéspedes el uso de billeteras virtuales como Google pay, Apple pay o tarjetas virtuales de prepago, para que sus datos bancarios no se vean comprometidos en ataques similares.

El siguiente tipo de ataque que se va analizar es el "*ransomware*", definido por Kaspersky como un programa de software malicioso que infecta tu computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema. Este tipo de malware es un sistema criminal para ganar dinero que se puede instalar a través de enlaces engañosos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web. El ransomware tiene la capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña.

El caso a analizar relacionado con este ataque es el del hotel Romantik Seehotel Jaegerwirt, de 4 estrellas, en Austria. En el año 2016 el hotel sufrió el ataque de un ransomware el cual paralizó el servicio de las llaves electrónicas, entre otros servicios, dejando a 180 clientes sin acceso a su habitación y al hotel sin poder hacer nada. Según las declaraciones del director del hotel pagaron los 1500 € que los criminales les exigían al igual que otros colegas suyos habían hecho anteriormente. Tras el pago de la suma reclamada y durante la reestructuración de su red de seguridad que costó varios miles de euros y de la cual el seguro no se quiso hacer cargo, descubrieron que los atacantes habían dejado una puerta trasera en su sistema con el fin de volver a infectarles.
La mejor forma de prevenir este tipo de ataques es mediante la correcta formación en ciberseguridad del personal.

A continuación, vamos a ver el "*DDOS o Denegación Distribuida de Servicio*", definido por Kaspersky como un ataque que aprovecha los límites de capacidad específicos que se aplican a cualquier recurso de red, tal como la infraestructura que habilita el sitio web de la empresa. El ataque DDOS envía varias solicitudes al recurso web atacado, con la intención de desbordar la capacidad del sitio web para administrar varias solicitudes y evitar que este funcione correctamente.

El caso seleccionado que guarda relación con el ataque DDOS es el que sufrió la web de la cadena Trump Hotels en 2017, esto fue descubierto por el corresponsal del Washington Post Philip Bump que colgó la siguiente captura de pantalla en su perfil de Twitter:



El siguiente error aparecía al intentar entrar a la web, traduciéndose en la incapacidad por parte de los clientes y potenciales clientes de usar cualquier funcionalidad que esta ofrezca.
Una posible contramedida para estos ataques es la contratación de los servicios de empresas como Cloudflare que se encargan de analizar las peticiones que está recibiendo el sistema y discernir si son reales o pertenecen a un ataque DDOS.

En cuarto lugar, tenemos los "*Point of sale attacks*" o ataques al punto de venta. Para ello, lo primero que debemos saber es que son los dispositivos de punto de venta. según Broadcom, los puntos de venta, son los sistemas de tiendas u otros establecimientos donde los clientes realizan los pagos. En la actualidad estos sistemas son capaces de soportar distintos métodos de pago y están en constante evolución.
El ataque, en este caso, consiste en inyectar malware en el dispositivo que reenvía información bancaria de los clientes a los delincuentes.

Un caso real real relacionado con este tipo de ataque es lo que sucedió en la cadena Omni, entre otras como Hilton o Hyatt, en 2016 cuando un grupo de ciberdelincuentes tomó el control de los POS de 49 de los 60 hoteles de la cadena y estuvo robando información bancaria de los clientes durante 6 meses antes de ser descubiertos.

Para evitar este tipo de ataque, igual que con el phishing se recomienda a los clientes el uso de billeteras electrónicas como Google pay, Apple pay o tarjetas virtuales de prepago.

Finalmente trataremos el último ataque y probablemente el más sofisticado, este es "*Darkhotel*". Kaspersky lo define como una combinación de spear phishing y malware peligroso diseñada para capturar datos confidenciales.

El método seguido por los criminales se puede ver claro en el siguiente gráfico ofrecido por Kaspersky, empresa descubridora de Darkhotel.

Tabla 34.- Método del ataque Darkhotel

Darkhotel se calcula que está activa desde 2007 y fue descubierto por expertos de Kaspersky en 2014, durante esos 7 años hay constancia de que ha obtenido información de altos cargos de empresas de 13 países, por lo menos.

La forma recomendada para protegerse de este ataque se puede resumir en 3 directrices, mantener el software actualizado, usar VPNs en redes y WiFi públicas y tener una actitud escéptica ante cambios y mensajes poco habituales en los dispositivos.

Para concluir, cabe remarcar "*la importancia de la seguridad de los datos de los clientes".* Para ello, tomamos como referencia el caso de la empresa Marriott que recibió una multa de 110 M € por parte de la oficina del comisionado de información de Reino Unido, por violar el reglamento general de protección de datos europea tras la exposición de la brecha de datos de los clientes de su filial Starwood. Esta es la tercera mayor brecha de datos, hasta la fecha.

5.2. Identificación de riesgos

Para identificar los riesgos posibles en cada servicio se va a seguir la siguiente metodología: documentar una serie de ataques posibles a cada uno de los servicios con fallos explotables conocidos y recogidos en el informe Percepción y Uso de la Tecnología por el Cliente 4.0, en el sector hotelero del ITH, analizado en el punto 4 de este trabajo.

En primer lugar, la "***fase de inspiración***", que contaba con 2 servicios, la presencia en buscadores y en redes sociales.
En el primer caso un atacante malintencionado podría hacer uso de técnicas de blackhat seo, definido por Kaspersky como el hecho de mejorar el posicionamiento web haciendo uso de técnicas no aprobadas o prohibidas por los buscadores, para posicionar una web falsa por encima de la real para engañar a los posibles clientes.
En el caso de las redes sociales se puede ver una técnica muy parecida a la anterior, Blackhat social media que tiene la misma intención que en el caso anterior.

Seguidamente tenemos la **"*fase de planificación***" en la cual primeramente está la web del hotel, cuya seguridad puede ser vulnerada mediante técnicas de hacking web para obtener datos de los clientes o incluso llegar a vulnerar más servicios si el hotel no tiene un plan de ciberseguridad adecuado. En este caso también podemos incluir la falsa web posicionada anteriormente mediante blackhat seo para estafar a los clientes, esto es conocido como phishing.
En la misma fase encontramos los chats directos, ya sean falsos o verdaderos que hayan sido comprometidos y que pueden ser usados por los criminales para obtener datos personales sobre los clientes mediante técnicas de ingeniería social.
Finalmente encontramos los tours mediante realidad virtual, los cuales pueden parecer inofensivos pero como advierte Herschel Jawitz, CEO Jawitz Properties una de las mayores inmobiliarias de Sudáfrica es posible mostrar mucha más información de lo que se quiere con estos tours hecho que puede facilitar mucho el trabajo a posibles delincuentes que tengan intención de realizar robos o otros actos ilícitos en el hotel

En la "***fase de contratación***" no aparecen tecnologías que no se hayan mostrado con anterioridad por lo que se va a omitir.

En la "***cuarta fase o Estancia***" es en la que más servicios se ofrecen, algunos que en la actualidad no suponen un problema de seguridad aunque se vean comprometidos por lo que se va a hacer un repaso por los que más problemas de seguridad podrían suponer:

En primer lugar tenemos los puestos de carga de móvil, estos son muy susceptibles a un ataque conocido como juice jacking. Esta práctica consiste en que los criminales carguen algún tipo de malware a la estación de carga que infecta a los dispositivos que se conecten a ella.

La siguiente tecnología son las llaves digitales, estas están en los smartphone de los clientes para una mayor comodidad. Cabe recalcar los problemas que pueden derivar de un fallo en este sistema como se ha visto en el caso del hotel austriaco del punto 5.1 y que los problemas relacionados con las llaves no son puramente con las digitales. En el caso de las cerraduras que se abren mediante tarjeta, un desarrollador de la empresa mozilla demostró en 2012 que con apenas 50 dolares de presupuesto y unas mínimas habilidades de programación es posible abrir al menos 1 de cada 4 puertas de hoteles que utilicen esta tecnología.
Volviendo a la tecnología que nos atañe, las llaves digitales pueden parecer más seguras que sus predecesoras pero aun así tienen vulnerabilidades que pueden ser explotadas como demostraron los investigadores alemanes Ray y Michael Huebler en 2019.

El siguiente servicio ofrecido por los hoteles que se va analizar es el chromecast, un dispositivo de google que permite al usuario enviar contenido desde su smartphone o tablet a una TV. En el año 2018 el investigador Amador Aparicio de la Fuente publicó un caso de uso de como obtuvo el control total del dispositivo durante su estancia en un hotel.

Tras ver el chromecast la siguiente tecnología similar a esta que señala el estudio del ITH son las smart TV sobre las cuales también se ha demostrado que es posible tomar el control total sobre ellas incluso accediendo al micrófono y cámara que algunos modelos llevan integrados.

Otro servicio tecnológico ofrecido por hoteles es el sistema de domótica en sus habitaciones, con esto los clientes pueden regular el termostato, manejar las persianas o las luces desde el hotel o incluso desde cualquier otro punto con una conexión a internet, una mala configuración de estos dispositivos puede llevar al control total de los dispositivos de todas las habitaciones por parte de una persona ajena como demostró el español Jesús Molina en el hotel de 5 estrellas St. Regis Shenzhen en China.

Últimamente también se ha popularizado, el préstamo de tablet por parte del hotel y si estas no reciben un mantenimiento como es debido después de cada cliente es posible que se haya instalado algún software en ellas para robar información de los clientes que las usen. Parecido a este es llamativo el caso del Handy Phone, un smartphone ofrecido por algunos hoteles con el que los huéspedes internacionales pueden hacer llamadas internacionales y tener una conexión a internet sin incurrir en grandes gastos. El teléfono en cuestión es una versión del modelo Infocus m808 modificada por la empresa de Hong Kong Tink labs, el problema es que estos teléfonos cuentan con unas versiones de Android totalmente desactualizadas y las cuales cuentan con vulnerabilidades públicas que dejan el terminal y sus datos totalmente expuestos.

Otra tecnología que se suele ofrecer en hoteles son aplicaciones propias con las apps de menú diario o de guía cultural, estas deben estar diseñadas de tal forma que almacenen de forma segura los datos obtenidos de los clientes y no supongan brechas de seguridad en sus dispositivos.

Finalmente el wifi, la tecnología esencial que debe ofrecer el alojamiento para la mayoría de clientes y una de las que más problemas de seguridad puede suponer.
En primer lugar, los delincuentes pueden engañar a los clientes para que se conecten a una red wifi maliciosa que simula ser la del hotel y sobre la cual tienen total control. Para ello utilizan dos técnicas diferentes, Honeypot y Evil Twin, en la primera el atacante crea una red abierta con un nombre susceptible de que el cliente se conecte y en el segundo el atacante crea una red con el mismo nombre que la del hotel mientras deniega el servicio de este hecho, que provoca que todos los clientes que se conecten automáticamente a la red del hotel entren en la red maliciosa.
Una vez la víctima se conecta a la red del delincuente o éste se conecta a la red poco segura del hotel, lleva a cabo un ataque conocido como Man in the middle mediante el que el atacante es capaz de ver todo el tráfico de la víctima incluyendo sus datos personales e incluso podría derivar en accesos ilícitos a los dispositivos conectados a la red.

En la fase quinta y última, **la fase de compartir**, encontramos 3 servicios, dos de los cuales ya se ha hablado anteriormente y uno, las encuestas internas, donde no se ha detectado ninguna vulnerabilidad.

Así pues, en este apartado hemos identificado los riesgos más frecuentes, dentro de las distintas fases enumeradas para el sector hostelero. Cabe apreciar que la fase donde más riesgos se han encontrado es la fase de estancia aunque también parece lógico porque es la que mayor servicios registra, le sigue en incidencias de riesgo, la fase de planificación y la fase de inspiración.

5.3. Recomendaciones de seguridad según ISO27001/2

Norma ISO 27002

La ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013.

Los requisitos establecidos en esta Norma Internacional son genéricos y se pretende que sean aplicables a todas las organizaciones, sin importar su tipo, tamaño o naturaleza. Además, permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001

Esta norma internacional especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información en el contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información a la medida de las necesidades de la organización.

Con estas recomendaciones se busca proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan.

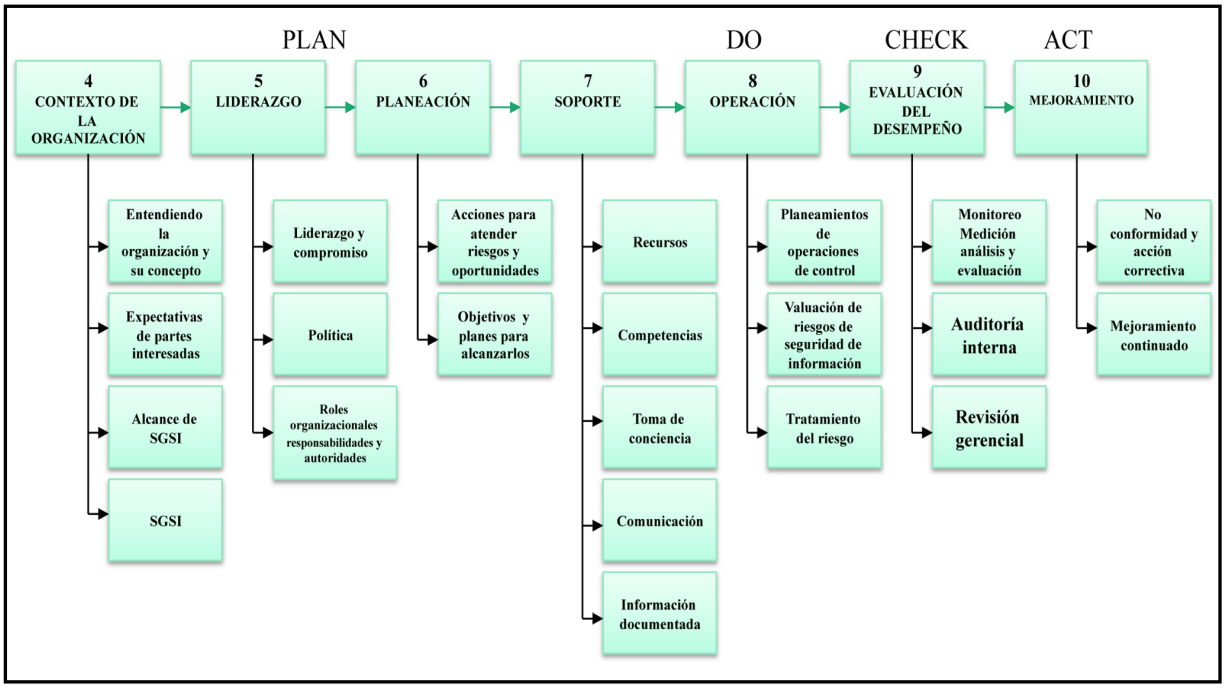
Las medidas de seguridad a implementar se presentan bajo la forma de políticas, procedimientos e implementación técnica. La mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales necesarias para prevenir violaciones de la seguridad.

La implementación de esta norma para la seguridad de la información tiene una serie de ventajas como: cumplir con los requerimientos legales, obtener una ventaja comercial y mejores costos y sobre todo una mejor organización de la empresa.

Para implementar ISO 20071 se tiene que realizar una serie de pasos que como observamos en el esquema siguiente podemos agrupar en: contexto de la organización, liderazgo, planeación o planificación, apoyo o soporte, operación, evaluación del desempeño y mejora.

Y además en este esquema también, se interrelacionan con las 4 fases del sistema de gestión: planificación (PLAN), implementar (DO), revisión (CHECK) y mantenimiento y mejora (ACT).

Tabla 35. Pasos de ISO 20071 y fases de su desarrollo



Así pues los pasos que desarrolla el ISO 20071 son:

4.- CONTEXTO DE LA ORGANIZACIÓN

Dentro del **contexto de la organización**, en primer lugar, se debe tener un *conocimiento claro de la organización*. Para ello, se determinarán los asuntos internos y externos que sean relevantes para conseguir los objetivos. También se deben precisar *las necesidades y expectativas de las partes* interesadas y los requisitos de las mismas, así como determinar el *alcance del sistema de seguridad* de la información. Para determinar este alcance, la organización deberá determinar los límites y la aplicabilidad del sistema de seguridad en la organización. Se deberán tener en cuenta al menos, los asuntos internos y externos, los requisitos de las partes interesadas en la seguridad y las interfaces y dependencias entre las actividades desempeñadas por la organización. Y por último, y como elemento clave se debe definir y precisar el ***Sistema de Gestión de la Seguridad de la información (SGSI)*** que además se deberá implementar, mantener y mejorar de manera continua.

5.- LIDERAZGO

La Dirección deberá demostrar su **liderazgo** *y compromiso*, garantizando el establecimiento de objetivos de la seguridad compatibles con la organización. Además debe garantizar los recursos necesarios para desarrollar el sistema de gestión de la información, fomentar la comunicación, garantizar que la seguridad logre los resultados esperados y desde luego, promover la mejora continua.

Respecto a la *política*, hay que señalar que ha de ser la dirección quien debe establecer una política de seguridad que sea adecuada al propósito y objetivos de la organización, que incluya el compromiso de satisfacer los requisitos relacionados con la seguridad y que contribuya al proceso de mejora continua. Además esta política debe estar comunicada a todas las partes interesadas.

Y por último se debe garantizar que se asigne y comunique las *responsabilidades y autoridad* para los roles relacionados con la seguridad de la información.

6.- PLANEACIÓN O PLANIFICACIÓN

La Organización realizará la **planificación** de la seguridad de la formación, evaluando los riesgos, realizando un tratamiento de los riesgos y marcando unos objetivos de seguridad de la información y planificación para alcanzarlos.

La *evaluación de los riesgos y su tratamiento* se debe considerar el eje central de este Sistema de la Gestión de la Seguridad de la Información (SGSI). Para ello, es necesario elegir una metodología adecuada que tenga al menos los siguientes puntos:

- Identificar los "**activos de Información**" y sus responsables, entendiendo por activo todo aquello que tiene valor para la organización, incluyendo soportes físicos (edificios o equipamientos), intelectuales o informativas (ideas, aplicaciones, proyectos…) así como la marca, la reputación etc.
- Identificar las "**vulnerabilidades**" de cada activo: aquellas debilidades propias del activo que lo hacen susceptible de sufrir ataques o daños.
- Identificar las "**amenazas**": Aquellas cosas que puedan suceder y dañar el activo de la información, tales como desastres naturales, incendios o ataques de virus, espionaje etc.
- Identificar los "**requisitos legales**" y contractuales que la organización está obligada a cumplir con sus clientes, socios o proveedores.
- "**Identificar los riesgos**": Definir para cada activo, la probabilidad de que las amenazas o las vulnerabilidades propias del activo puedan causar un daño total o parcial al activo de la información, en relación a su disponibilidad, confidencialidad e integridad del mismo.
- "**Cálculo del riesgo**": Este se realiza a partir de la probabilidad de ocurrencia del riesgo y el impacto que este tiene sobre la organización (Riesgo = impacto x probabilidad de la amenaza). Con este procedimiento determinamos los riesgos que deben ser controlados con prioridad.
- "**Plan de tratamiento del riesgo**": En este punto estamos preparados para definir la política de tratamiento de los riesgos en función de los puntos anteriores y de la política definida por la dirección. En este punto, es donde seleccionaremos los controles adecuados para cada riesgo, los cuales irán orientados a :
    - Asumir el riesgo
    - Reducir el riesgo
    - Eliminar el riesgo
    - Transferir el riesgo

Además en la planificación, debemos tener en cuenta, *los objetivos de seguridad de la información* y la planificación para alcanzarlos. Para ello, los objetivos deberán: ser consistentes con la política de seguridad de la información, ser medible- si es posible, tener en cuenta los requisitos de seguridad y los resultados de la evaluación y tratamiento de riesgos, ser comunicados y actualizarse- si fuera necesario.
Y al planificar estos objetivos, la organización deberá determinar: qué deberá hacer, qué recursos necesitará, quién será el responsable, cuándo será alcanzado dicho objetivo y cómo medirá los resultados.

7.- APOYO O SOPORTE
La organización deberá tener en cuenta el **apoyo o soporte** que necesita para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la información.
Para ello, deberá determinar y proporcionar los *recursos necesarios*, así como las *competencias* necesarias de las personas que harán el trabajo, recibiendo la formación adecuada, como capacitación, tutoría, reasignación de empleados o subcontratación.
Además, de *concienciar* a las personas que van a desempeñar la función para que partan y compartan la política de seguridad.
Dentro de este apoyo, se considera fundamental la *comunicación* al personal del sistema de gestión de seguridad, por medio de comunicaciones internas y externas. Se tendrá que determinar qué, cuándo , con quién y quién se debe realizar esta comunicación para que sea efectiva.
Pero no menos importante y complementario al anterior, es que tipo de *documentación* se debe elaborar.
Para elaborar esta documentación se deberá partir de la Norma Internacional y de la organización del SGSI de la propia organización. Además es fundamental que sea creativa y que esté actualizada y disponible.

8.- OPERACIÓN
En este apartado de **operación**, tendremos en cuenta *la planificación y control operacional*, para ello la organización deberá planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos del SGSI e implementar las acciones y planes correspondientes.
Así mismo, deberá mantener información documentada de forma que se garantice que lo planificado se está llevando a cabo y además deberá mantener un control sobre los cambios planificados y los procesos tercerizados.
Además se debe realizar una *evaluación de los riesgos de seguridad* de la información e implementar el *plan de tratamiento adecuado a dichos riesgos*.

9.- EVALUACIÓN DEL DESEMPEÑO
Para la evaluación del **desempeño**, se utilizarán: el monitoreo, medición, análisis y evaluación, las auditorías internas y la revisión por parte de la dirección.
Respecto al *monitoreo, medición, análisis y evaluación*, la organización deberá determinar las necesidades que deben ser monitoreadas y sometidas a medición, incluyendo los procesos y controles de la seguridad de la información, los métodos a utilizar en el monitoreo, la medición, el análisis y la evaluación, cuándo y quién deberá realizarlos y cuándo y quién deberá analizarlos.
Y además, lo que consideramos muy importante, deberá conservarse esta evaluación como "evidencia" para futuros procesos.
Respecto a las *auditorías internas,* la organización deberá dirigirlas en intervalos periódicos planificados y tener siempre en cuenta auditorias previas. Para que una auditoría sea eficaz se deben definir los criterios y alcance de la misma, seleccionar a los auditores, garantizar la comunicación de los resultados y conservar los resultados como evidencia de futuras auditorías
Y respecto a la *revisión por parte de la dirección,* deberá incluir el estatus de las acciones de las anteriores
Revisiones, los cambios en los asuntos externos e internos que tuvieron relevancia para el SGSI, la retroalimentación sobre el desempeño de la seguridad de la información, el cumplimiento de los objetivos de seguridad de la información, la retroalimentación de las partes interesadas, los resultados de la evaluación de los riesgos y las oportunidades de mejora continua.

10.- MEJORA
La organización deberá *mejorar de manera continua* la idoneidad, adecuación y efectividad del SGSI. Pero puede ocurrir que haya una *no conformidad* y entonces se tiene que aplicar una *acción correctiva.* Cuando ocurre una no conformidad, la organización debe: reaccionar ante ella, tomar acciones para controlarla y corregirla y asumir las consecuencias. Además debe evaluar la necesidad de acción para eliminar la no conformidad mediante una revisión de las misma, determinando las causas e implementando las acciones necesarias para corregirlas, que deberán ser implementadas como cambios al SGSI.

Definidos los pasos que desarrolla el ISO 20071, a continuación vamos a enumerar brevemente la FASES que lo desarrollan. Son las siguientes:

a) La fase de planificación **(PLAN)**: esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad.
b) La fase de implementación **(DO)**: esta fase implica la realización de todo lo planificado en la fase anterior.
c) La fase de revisión **(CHECK)**: el objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos "canales" y verificar si los resultados cumplen los objetivos establecidos.
d) La fase de mantenimiento y mejora **(ACT)**: el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

El ciclo de estas cuatro fases nunca termina, todas las actividades deben ser implementadas cíclicamente para mantener la eficacia del SGSI.

Norma ISO 27002

La norma ISO 27002 fue publicada por primera vez en 2005 como un cambio de nombre de la norma ISO 17799 la cual estaba basada en el British Standard BS 7799-1 de Reino Unido. Su publicación fue conjunta con la de la norma ISO 27001 debido a la naturaleza complementaria de ambos documentos.

En la ISO/IEC 27002 se extiende la información que aparece el anexo A de la ISO/IEC 27001-2013. En esta ISO se ofrecen recomendaciones de las mejores prácticas en la gestión de la seguridad de la información para cualquier empresa independientemente de sus características asegurando siempre la confidencialidad, integridad y disponibilidad de los datos.

Así pues, dentro de ISO/IEC 27002 se describen los dominios de control y los mecanismos de control, que pueden ser implementados dentro de una organización, siguiendo las directrices de ISO 27001. En esta nueva versión de la norma se encuentran los controles que buscan mitigar el impacto o la posibilidad de ocurrencia de los diferentes riesgos a los cuales se encuentra expuesta la organización.

Con la actualización de esta norma las organizaciones pueden encontrar una guía que sirva para la implementación de los controles de seguridad de la organización y de las prácticas más eficaces para gestionar la seguridad de la información.

La ISO/IEC 27002 se divide en 14 áreas generales ,que se van a nombrar a continuación, junto con sub áreas más específicas e indicadores para evaluar el desempeño de cada una. Las áreas son:
- Políticas de seguridad de la información
- Organización de la seguridad de la información
- Seguridad de los recursos humanos
- Gestión de los Activos
- Control de acceso
- Criptografía

- Seguridad física y medioambiental
- Seguridad de las operaciones
- Seguridad de las comunicaciones
- Sistema de adquisición, desarrollo y mantenimiento
- Relaciones con los proveedores
- Información de gestión de incidentes de seguridad
- Los aspectos de seguridad de información de la gestión de la continuidad del negocio
- Conformidad.

Existen cambios en la ubicación de puntos concretos que se encuentran en secciones y apartados distintos pero también existen dominios de control nuevos que llaman la atención como la "criptografía" donde se incluyen todos los controles criptográficos sugeridos para la organización.
También, señalar que, existen versiones específicas de la norma ISO/IEC 27002, dirigidas a diferentes tipos de empresas de distintos sectores, como salud, manufacturas o el sector financiero.

Como conclusión del punto señalar que, hemos estudiado y revisado la estructura del ISO27001, una normativa internacional que permite establecer un Sistema de Gestión de la Seguridad de la información (SGSI) que las organizaciones deberán implementar, mantener y mejorar de manera continua. Se han descrito los pasos: contexto de la organización, liderazgo, planeación o planificación, apoyo o soporte, operación, evaluación del desempeño y mejora para una mejor adecuación al planteamiento de la propuesta del punto siguiente. Incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información a la medida de las necesidades de la organización.
Y además, se han enumerado las fases que constituyen un verdadero ciclo DEMING o de mejora continua.

6.- PROPUESTA DE SEGURIDAD PARA UNA PYME HOTELERA SEGÚN LA ISO 27001

Este apartado final se estructura en dos puntos fundamentales, el análisis de riesgo previo y la propuesta propiamente dicha que hemos titulado "recomendaciones para la seguridad de la PYME hotelera mediante la aplicación de la ISO 27001"

6.1 Análisis de riesgos

Para el análisis de riesgo, analizaremos el inventario de activos básicos, las dimensiones de seguridad y el análisis de amenazas.

6.1.1 Inventario de activos

Para realizar el análisis del inventario de activos vamos a seguir las recomendaciones de la metodología Magerit, creada por el Consejo Superior de Administración Electrónica del Gobierno de España.

Según Magerit hay 10 tipos de activos: Hardware, Software, Servicios, Personal, Datos, Redes de Comunicación, Claves criptográficas, Soportes de información, Equipamiento auxiliar e Instalaciones.

De entre los 10 tipos de activos, se han seleccionado los 6 primeros y se han descartado los 4 últimos por el bajo aporte a la ejemplificación del objetivo del trabajo.

A continuación, se incluyen las tablas relacionadas con los seis primeros, indicando en cada una de ellas el tipo de activo y los activos que posee la empresa de este tipo.

Tabla 36. Tablas para el análisis del inventario de activos

Tipo	Activo
Hardware	Dispositivos para copias de seguridad
	Ordenadores
	Dispositivos de almacenamiento
	Firewalls
	Teléfonos móviles
	Tablets
	Routers
	Switches
	Smart TV
	Instalación Domótica

Tipo	Activo
Software	Sistemas Operativos
	Sistema de backup
	Sistema Gestión Bases de Datos
	Dispositivos de almacenamiento
	Ofimática
	Antivirus
	Cliente correo electrónico

Tipo	Activo
Servicios	Web
	Aplicación
	Correo electrónico
	Gestión de identidades
	Gestión de privilegios

Tipo	Activo
Personal	Usuarios Internos
	Usuarios externos
	Administrador de sistemas
	Subcontratas

Tipo	Activo
Datos	Copias de respaldo
	Datos de Gestión interna
	Credenciales
	Datos de validación de credenciales
	Registro de actividad (logs)

Tipo	Activo
Redes de Comunicación	Red telefónica
	Red inalámbrica
	Telefonía móvil
	Red local
	Internet

Estos son los activos que tiene la empresa propuesta en el punto 3.4

6.1.2 Dimensiones de valoración de los activos

Tras haber recopilado todos los activos sensibles de la empresa en el punto anterior, se procede a describir las 5 dimensiones de valoración de los activos que se especifican en la tabla adjunta: disponibilidad, integridad de los datos, confidencialidad de la información, autenticidad y trazabilidad.
Cada servicio que ofrecen los activos pueden tener una o varias de estas dimensiones. Pero además estas dimensiones pueden verse alteradas por la afección de la materialización de una amenaza.

Tabla 37. Dimensiones de valoración de los activos

Dimensiones de valoración de los activos	
[D] Disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
[I] Integridad de los datos	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[C] Confidencialidad de la información	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
[A] Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008] (Importancia del No Repudio)
[T] Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008] (Auditabilidad)

6.1.3 Análisis de amenazas

Cada uno de los activos descritos anteriormente, puede verse afectado por una serie de amenazas alterando alguna o varias de las dimensiones de seguridad que garantiza. A continuación se nombran las amenazas clasificadas por categorías según aparecen en la metodología Magerit. Para consultar a qué tipo de activo y dimensión afecta cada una, en el anexo 2 se encuentra la explicación detallada de cada amenaza que ofrece Magerit.

En algunos casos sucede que un mismo problema puede originarse por un error o por un ataque, en la última página del anexo 2, anteriormente citado, se analiza la casuística y se traza el paralelismo entre acciones deliberadas o errores.

[N] Desastres naturales. Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

- [N.1]Fuego
- [N.2]Daños por agua
- [N.*]Desastres naturales

[**I] De origen industrial**. Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
Origen: Natural (accidental)

- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación mecánica
- [I.4] Contaminación electromagnética
- [I.5] Avería de origen físico o lógico
- [I.6] Corte de suministro eléctrico
- [I.7] Condiciones inadecuadas de temperatura o humedad
- [I.8] Fallo de servicios de comunicaciones
- [I.9] Interrupción de otros servicios y suministros esenciales
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados. Fallos no intencionales causados por las personas.
Origen: Humano (accidental)

- [E.1] Errores de los usuarios
- [E.2] Errores del administrador
- [E.3] Errores de monitorización
- [E.4] Errores de configuración
- [E.7] Deficiencias en la organización
- [E.8] Difusión de SW dañino
- [E.9] Errores de [re]-encaminamiento
- [E.10] Errores de secuencia
- [E.14] Escapes de información
- [E.15] Alteración accidental de la información
- [E.18] Destrucción de la información
- [E.19] Fugas de información
- [E.20] Vulnerabilidades de los programas (SW)
- [E.21] Errores de mantenimiento / actualización de programas (SW)
- [E.23] Errores de mantenimiento / actualización de equipos (HW)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Pérdida de equipos
- [E.28] Indisponibilidad del personal

[A] Ataques intencionados. Fallos deliberados causados por las personas.
Origen: Humano (deliberado)

- [A.3] Manipulación de los registros de actividad (log)
- [A.4] Manipulación de la configuración
  [A.5] Suplantación de la identidad del usuario
  [A.6] Abuso de privilegios de acceso
- [A.7] Uso no previsto
- [A.8] Difusión de software dañino
- [A.9] [Re-]encaminamiento de mensajes
- [A.10] Alteración de secuencia
- [A.11] Acceso no autorizado
- [A.12] Análisis de tráfico
- [A.13] Repudio
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación deliberada de la información
- [A.18] Destrucción de información
- [A.19] Divulgación de información
- [A.22] Manipulación de programas
- [A.23] Manipulación de los equipos
- [A.24] Denegación de servicio
- [A.25] Robo
- [A.26] Ataque destructivo
- [A.27] Ocupación enemiga
- [A.28] Indisponibilidad del personal
- [A.29] Extorsión
- [A.30] Ingeniería social (picaresca)

Con este apartado hemos desarrollado las etapas que consideramos imprescindibles, el inventario de activos, las dimensiones de valoración de los activos y el análisis de amenazas más significativas. A continuación y como finalización del trabajo, establecer unas recomendaciones de seguridad para un PYME hotelera aplicando la ISO 27001 y que desarrollaremos a continuación.

6.2 Recomendaciones para la seguridad de la PYME hotelera mediante la aplicación de la ISO 27001

En este apartado se van a dar una serie de recomendaciones (*expresadas en rojo*) orientadas a una Pyme hotelera como la descrita en el apartado 3.4. Para ello, vamos a basarnos en el anexo A de la ISO 27001, donde se detallan los puntos clave a controlar para maximizar la seguridad de cualquier empresa.

A.5 Políticas de seguridad de la información		
A.5.1 Dirección de Gestión de Seguridad de la Información		
Objetivo: Proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requerimientos del negocio y las leyes y reglamentos pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	El hotel debe de contar con unas políticas de seguridad de la información aprobadas por la dirección y conocidas por todos los empleados.
A.5.1.2	Revisión de las políticas de información seguridad	Las políticas de seguridad deben de ser revisadas de manera planificada en intervalos de tiempo prudenciales para asegurar la eficacia de estas con el paso del tiempo.

A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades de seguridad de información	Las responsabilidades para la seguridad de la información deben ser definidas y asignadas al responsable que establezca la dirección.
A.6.1.2	Segregación de deberes	Dentro de las limitaciones surgidas de ser una Pyme se distribuirán las tareas entre el personal del hotel para evitar las oportunidades de un uso indebido. Se podrán utilizar registros automatizados o controles de seguimiento.
A.6.1.3	El contacto con las autoridades	Se deben mantener los contactos adecuados con las autoridades pertinentes, como la agencia de protección de datos.
A.6.1.4	El contacto con los grupos de interés especial	Se deben mantener los contactos adecuados con los grupos de interés u otros foros de seguridad especializadas y las asociaciones profesionales para estar actualizados permanentemente.
A.6.1.5	Seguridad de la información en la gestión de proyectos	En el caso de realizar un nuevo proyecto se deberá garantizar la seguridad de la nueva información, siguiendo los procedimientos establecidos por los proyectos en funcionamiento.

A.6.2 Los dispositivos móviles y el teletrabajo		
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.		
A.6.2.1	Política de dispositivo móvil	Los teléfonos móviles del personal deberán de usar siempre una red diferente a la de administración del hotel y estará prohibido portarlos en las áreas especialmente delicadas.
A.6.2.2	Teletrabajo	Se teletrabajará mediante el uso de VPN + Escritorio remoto. Si es posible se usarán dispositivos corporativos y si no se seguirá una política "Bring Your Own Device" siguiendo las recomendaciones del "incibe".

A.7 La seguridad de los recursos humanos		
A.7.1 Antes de empleo		
Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean adecuados para las funciones para las que se consideran.		
A.7.1.1	Selección	Se llevarán a cabo una serie de medidas de seguridad en el proceso de selección como comprobación de antecedentes, de la identidad y veracidad del CV. Estos elementos se completarán con pruebas para verificar sus competencias.
A.7.1.2	Términos y condiciones de empleo	Los acuerdos contractuales con los empleados y contratistas deberán declarar responsabilidades de sus actuaciones para garantizar la seguridad de la información.
A.7.2 Durante el empleo		
Objetivo: Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información.		
A.7.2.1	Responsabilidad de la dirección	Todos los empleados deberán aplicar las políticas de seguridad de la información definidas por la dirección.
A.7.2.2	Concienciación sobre la seguridad de la información, la educación y la formación	Todos los empleados deberán recibir formación y actualizaciones periódicas sobre seguridad de la información. "incibe" ofrece soluciones gratuitas para empresas.
A.7.2.3	Proceso disciplinario	Habrá un proceso disciplinario formal y comunicado en lugar de tomar medidas arbitrarias contra los empleados que hayan cometido una violación de la seguridad de la información. El proceso asegurará que la infracción se ha cometido y la respuesta será a la infracción cometida.
A.7.3 Finalización o cambio de empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambiar o terminar el empleo.		

A.7.3.1	La terminación o el cambio de responsabilidades laborales	Al finalizar o cambiar de empleo, el empleado deberá proteger la información adquirida en el desarrollo de su trabajo, tal y como se debe indicar en las cláusulas del contrato inicial.

A.8 Gestión de activos		
A.8.1 La responsabilidad de los activos		
Objetivo: Identificación de los activos de la organización y definir las responsabilidades de protección adecuados.		
A.8.1.1	Inventario de activos	Los activos asociados a las instalaciones de procesamiento de información y la información deben ser identificados e inventariados.
A.8.1.2	La propiedad de los activos	Los activos mantenidos en el inventario serán propiedad de la empresa.
A.8.1.3	El uso aceptable de los activos	Deben definirse, documentarse e implementarse unas normas que aseguren el correcto uso de los activos
A.8.1.4	Retorno de los activos	Todos los empleados y los usuarios externos deberán devolver todos los activos de la organización en su poder a la terminación de su empleo, contrato o acuerdo.
A.8.2 Clasificación de la Información		
Objetivo: Garantizar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.		
A.8.2.1	Clasificación de la información	La información se clasifica según los requisitos legales, su valor, la criticidad, sensibilidad a la divulgación o modificación no autorizada.
A.8.2.2	Etiquetado de la información	La información deberá ser etiquetada de acuerdo al esquema de clasificación de la información aprobada por la empresa.
A.8.2.3	Manipulación de los activos	El manejo de los activos deberán desarrollarse según los acuerdos especificados en la clasificación de la información aprobada por la empresa.
A.8.3 Manipulación de soportes		
Objetivo: Evitar la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los soportes.		
A.8.3.1	Gestión de soportes extraíbles	Se seguirán las recomendaciones del “incibe” para el uso de dispositivos extraíbles en entornos empresariales.
A.8.3.2	La eliminación de los soportes	Los medios deberán ser desechados de forma segura cuando ya no sean necesarios, utilizando los procedimientos establecidos.

A.8.3.3	Traslado de soportes físicos	Los medios que contienen información sensible deberán estar protegidos contra el acceso no autorizado, mal uso o la corrupción durante su transporte.

A.9 Control de acceso		
A.9.1. Requerimientos de negocio para el control de acceso		
Objetivo: Limitar el acceso a personas no autorizadas a las instalaciones de procesamiento de la información y a la información.		
A.9.1.1	Política de control de acceso	Se establecerá una política de control de acceso, documentada y revisado, en base a los requisitos de seguridad definidos por la dirección
A.9.1.2	El acceso a las redes y los servicios de red	Los usuarios sólo deberán disponer de acceso a los servicios de red a los que han sido autorizados.
A.9.2 Gestión de acceso de usuario		
Objetivo: Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.		
A.9.2.1	Registro de usuarios y cancelación del registro	Se establecerá un control de usuarios con derechos de acceso y se darán de baja automáticamente al extinguir la relación laboral con el trabajador.
A.9.2.3	Gestión de derechos de acceso privilegiados	La asignación y uso de los derechos de acceso privilegiados serán restringidos y controlados por la dirección.
A.9.2.4	Gestión de la información de autenticación secreta de los usuarios	En el contrato u otro procedimiento se establecerá una cláusula de no revelación de autenticación personal
A.9.2.5	Revisión de los derechos de acceso de usuario	Los derechos de acceso de los usuarios a los activos serán revisados en intervalos regulares.
A.9.2.6	La eliminación o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y usuarios externos deberán de ser retirados a la terminación de su empleo, contrato o convenio
A.9.3 Responsabilidades del usuario		
Objetivo: Hacer a los usuarios responsables de salvaguardar su información de autenticación.		
A.9.3.1	El uso de información secreta de autenticación	Establecer unas normas básicas para asegurar el secreto de la información de autenticación.
A.9.4 Sistema de control y acceso a las aplicaciones		
Objetivo: Evitar el acceso no autorizado a los sistemas y aplicaciones.		

A.9.4.1	Restricción de acceso Información	El acceso a las funciones de administración estará oculto para los usuarios no autorizados.
A.9.4.2	Procedimientos de inicio de sesión de seguros	Las contraseñas de acceso debe de comunicarse de forma cifrada y la red debe registrar los intentos de acceso fallidos.
A.9.4.3	Sistema de gestión de contraseñas	El sistema de gestión de contraseñas debe asegurar que las contraseñas usadas sean robustas.
A.9.4.4	Uso de programas de utilidad privilegiados	El uso de programas que podrían ser capaces vulnerar las políticas de seguridad será restringido y estrechamente controlado.
A.9.4.5	Control de acceso al código fuente del programa	El acceso al código fuente de la aplicación debe estar restringido.

A.10 Criptografía		
A.10.1 Controles criptográficos		
Objetivo: Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y / o integridad de la información.		
A.10.1.1	Política sobre el uso de controles criptográficos	Se cifrarán aquellos medios extraíbles que transmitan información confidencial.
A.10.1.2	Gestión de claves	Se deberá desarrollar e implementar una política sobre el uso, la protección y la duración de las claves criptográficas

A.11 Seguridad física y ambiental		
A.11.1Áreas seguras		
Objetivo: Evitar el acceso no autorizado, el daño e interferencia de la información en las instalaciones de procesamiento de información de la organización.		
A.11.1.1	Perímetro de seguridad física	Se establecerán perímetros de protección para proteger áreas que contienen la información sensible mediante los dispositivos adecuados.
A.11.1.2	Controles de entrada físicas	Las zonas seguras se protegerán mediante controles de entrada adecuados para garantizar que se permite el acceso sólo al personal autorizado.

A.11.1.3	Asegurar oficinas, habitaciones e instalaciones	Uso de técnicas de enmascaramiento de nombres o actividades para asegurar las instalaciones varias.
A.11.1.4	La protección contra amenazas externas y ambientales	La protección física contra los desastres naturales, ataques maliciosos o accidentes estará diseñada en los correspondientes planes de continuidad de negocio o de prevención
A.11.1.5	Trabajar en zonas seguras	Se prohibirá el trabajo en el área segura sin supervisión
A.11.1.6	Zonas de entrega y carga	Los puntos de entrega y de carga deberán ser controlados en los distintos momentos.
A.11.2 Equipo		
Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.		
A.11.2.1	Ubicación y protección equipo	Los equipos deberán estar protegidos y situados en en un sitio que permita reducir los riesgos de las amenazas ambientales y oportunidades de acceso no autorizado.
A.11.2.2	Elementos de soporte	Se deberá cumplir con las especificaciones de los fabricantes y los requisitos legales establecidos en dichos elementos
A.11.2.3	Seguridad cableado	El cableado que transporta datos o el apoyo a los servicios de información, deberá ser protegido contra la intercepción de datos, interferencia o daños.
A.11.2.4	Mantenimiento de equipo	El mantenimiento del equipo deberá ser llevado a cabo por personal autorizado, siguiendo las recomendaciones del fabricante.
A.11.2.5	La eliminación de los activos	Los activos de datos, software o hardware serán eliminados por personal autorizado.
A.11.2.6	Seguridad de los equipos y activos fuera del establecimiento	Se aplicará una política de seguridad a los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de los locales del hotel. *(Políticas BYOD)*
A.11.2.7	Eliminación segura o reutilización de equipos	Todos los elementos del equipo que contienen medios de almacenamiento deberán ser verificados para asegurar que los datos sensibles y software con licencia se haya eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.
A.11.2.8	Equipamiento desatendido por el	Los usuarios deberán asegurarse de que el equipo desatendido tiene la sesión cerrada.

	usuario	
A.11.2.9	Política de pantalla y escritorio limpios	El escritorio deberá estar limpio de papeles y soportes de almacenamiento extraíbles y la pantalla del escritorio deberá estar lo más despejada posible.

A.12 La seguridad de Operaciones		
Procedimientos y responsabilidades operacionales A.12.1		
Objetivo: Garantizar operaciones correctas y seguras de instalaciones de procesamiento de información.		
A.12.1.1	Procedimientos operativos documentados	Los procedimientos operativos deberán ser documentados y puestos a disposición de todos los usuarios que los necesitan.
A.12.1.2	Gestión del cambio	Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de información y sistemas que afectan a la seguridad de información deberán ser controlados mediante un registro interno.
A.12.1.3	Gestión de la capacidad	El uso de los recursos será supervisado y se ajustará a las necesidades de capacidad del sistema para asegurar su correcto funcionamiento.
Protección A.12.2 del malware		
Objetivo: Asegurar que las instalaciones de la información y procesamiento de información están protegidas contra el malware.		
A.12.2.1	Controles contra el malware	Se llevarán a cabo controles de prevención y detección periódicos junto con una correcta formación al personal.
A.12.3 de copia de seguridad		
Objetivo: Evitar la pérdida de datos.		
A.12.3.1	Copia de seguridad de la información	Las copias de seguridad de la información, software se harán y se comprobará su integridad regularmente de acuerdo a la política definida.
A.12.4 Registro y monitoreo		
Objetivo: Registrar eventos y generar evidencia.		
A.12.4.1	El registro de eventos	Se realizará un registro de eventos que facilite ante un incidente su estudio. En general, se registrarán con regularidad.

A.12.4.2	Protección de la información de registro	La información de registro estará protegida contra la manipulación y acceso no autorizado y se guardará una copia de seguridad de ésta.
A.12.4.4	Sincronización de reloj	Los relojes de todos los sistemas de procesamiento de información se sincronizarán con una sola fuente de tiempo de referencia.
A.12.5 Control de del software operativo		
Objetivo: Garantizar la integridad de los sistemas operativos.		
A.12.5.1	Instalación de software en sistemas operativos	El software de los sistemas operativos deberán tener una licencia válida y mantenerse actualizado con las última actualizaciones de seguridad
A.12.6 Gestión vulnerabilidad técnica		
Objetivo: Prevenir la explotación de vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	El personal deberá ser consciente de las vulnerabilidades técnicas que pueden haber en los sistemas con los que trabaja y realizar escaneos periódicos de éstas.
A.12.6.2	Restricciones a la instalación de software	Excepto el administrador de red, el resto de usuarios no tendrán permisos para instalar software en los dispositivos del hotel.
A.12.7 Consideraciones de auditoría de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.		
A.12.7.1	Sistemas de información controles de auditoría	Las actividades de auditoría en los sistemas deberán ser programadas de forma que se asegure la máxima disponibilidad de estos.

A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de la seguridad de red		
Objetivo: Garantizar la protección de la información en las redes y sus instalaciones de apoyo de procesamiento de información.		
A.13.1.1	Controles de red	Las redes deberán ser gestionadas y controladas mediante controles de acceso y de privilegio, para proteger la información de los sistemas conectados a ellas.
A.13.1.2	Seguridad de los servicios de red	Los servicios de red deben ser prestados en la empresa o subcontratados deben ser identificados e incluidos en los acuerdos todos los mecanismos de seguridad, niveles de servicio y los requisitos de gestión.
A.13.1.3	La segregación en las redes	Se definirán varias redes entre las cuales encontramos la de clientes, personal y administración. Y en el caso de nuestro ejemplo una red para el sistema de domótica.

A.13.2 La transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de transferencia de información	Deberán definirse políticas para la transferencia segura de la información, incluyendo requisitos contra la intercepción, copia, modificación o destrucción de los datos.
A.13.2.2	Los acuerdos sobre la transferencia de información	Se deben acordar métodos seguros de transferencia de información entre la empresa y los interesados externos.
A.13.2.3	La mensajería electrónica	La información presente en la mensajería electrónica deberá ser protegida y firmada digitalmente cuando sea posible para garantizar su integridad.
A.13.2.4	Los acuerdos de confidencialidad y de no divulgación	Documentar y revisar los acuerdos de confidencialidad o no divulgación mantenidos con el personal y actores externos.

A.14 Sistema de adquisición, desarrollo y mantenimiento		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Garantizar que la seguridad informática sea una parte integral de los sistemas de información durante todo el ciclo de vida.		
A.14.1.1	Requisitos de seguridad: análisis y especificación	Los requisitos relacionados con la seguridad de la información se incluirán en los requisitos de los nuevos sistemas de información o mejoras a los sistemas de información existentes.
A.14.1.2	Asegurar los servicios de aplicación de redes públicas	La información involucrada con las aplicaciones que ofrecen servicios en redes públicas deberá estar protegida contra la actividad fraudulenta y modificación mediante el cifrado de las comunicaciones y uso de certificados digitales.
A.14.2 Seguridad en los procesos de desarrollo y soporte		
Objetivo: Asegurar que la seguridad de información se diseña e implementa dentro del ciclo de vida de desarrollo de sistemas de información.		
A.14.2.1	La política de desarrollo seguro	La aplicación desarrollada para la empresa ha sido desarrollada conforme a políticas de desarrollo seguro de software conforme a la ISO 33000 de calidad de procesos de desarrollo de software
A.14.2.6	Entorno de desarrollo seguro	Se debe establecer y proteger adecuadamente los entornos de desarrollo seguro, no sólo a los equipos sino también a la personas.
A.14.2.7	Desarrollo subcontratado	Si el desarrollo de la aplicación ha sido subcontratado, la empresa deberá supervisar el cumplimiento de los requisitos de seguridad.

A.14.2.8	Pruebas de seguridad del sistema	Durante el desarrollo de la aplicación se deberán llevar a cabo controles de funcionamiento y seguridad.
A.14.2.9	Pruebas de aceptación del sistema	Se establecerán pruebas de seguridad y funcionamiento para las nuevas aplicaciones y actualizaciones.
A.14.3.Los datos de prueba		
Objetivo: Garantizar la protección de los datos utilizados para la prueba.		
A.14.3.1	Protección de datos de prueba	Los datos de prueba no deben ser reales y en caso de no ser posible deberán seleccionarse cuidadosamente, protegerse y controlarse.

A.15 Relaciones con los proveedores		
A.15.1 Seguridad de la información en relaciones con los proveedores		
Objetivo: Garantizar la protección de los activos de la organización que sea accesible por los proveedores.		
A.15.1.1	Política de seguridad de la información para relaciones con los proveedores	Establecer protocolos para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización.
A.15.1.2	Abordar la seguridad dentro de acuerdos con proveedores	Todos los requisitos de seguridad de la información pertinentes serán establecidos y acordados con cada proveedor que pueden acceder, procesar, almacenar, comunicar, o proporcionar componentes de la infraestructura de TI de la empresa.
A.15.1.3	Cadena de la información y la tecnología de comunicación de suministro	Los acuerdos con los proveedores deberán incluir cláusulas concretas para hacer frente a los riesgos de seguridad de la información asociados a los servicios de información y tecnología de las comunicaciones y la cadena de suministro de productos.
A.15.2 Gestión de la prestación de servicios del proveedor		
Objetivo: Mantener un nivel acordado de seguridad de la información y la prestación de servicios en línea con los acuerdos con proveedores.		
A.15.2.1	Seguimiento y revisión de los servicios de proveedores	La empresa deberá controlar revisar y auditar regularmente, su lista de proveedores.
A.15.2.2	Gestión de cambios en los servicios de proveedores	Al cambiar los servicios de los proveedores, se deberá analizar el riesgo del nuevo escenario.

A.16 Información de gestión de incidentes de seguridad		
A.16.1Gestión de incidentes y mejoras de seguridad de la información		
Objetivo: Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	Se establecerán responsabilidades y procedimientos que garanticen una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Informar sobre los eventos de seguridad de información	Los eventos de seguridad de la información se comunicarán a través de canales de gestión apropiados lo antes posible.
A.16.1.3	Informes de debilidades de seguridad de la información	Se considera necesario que los empleados que utilizan los sistemas y servicios de información de la organización reporten cualquier debilidad de seguridad de información observada o sospechada en los sistemas.
A.16.1.5	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de información deberán recibir una respuesta conforme con los procedimientos documentados en la política de seguridad de la empresa.
A.16.1.6	Aprendiendo de los incidentes de seguridad de la información	Los conocimientos adquiridos desde el análisis y la resolución de los incidentes de seguridad de la información se utilizarán para reducir la probabilidad o el impacto de futuros incidentes y nos basaremos en el registro de los mismos.
A.16.1.7	El acopio de pruebas	La empresa debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como prueba para futuras sanciones o acciones legales.

A.17 Aspectos de seguridad de información de la gestión de la continuidad del negocio		
A.17.1 Continuidad de seguridad de la información		
Objetivo: La información sobre la continuidad de seguridad deberá estar integrada en los sistemas de gestión de continuidad de negocio de la organización.		
A.17.1.1	Planificación de la continuidad de seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas
A.17.1.2	La implementación de la continuidad de seguridad de la información	La empresa debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.

A.17.1.3	Verificar, revisar y evaluar la información de seguridad de continuidad	El hotel debe verificar los controles de seguridad establecidos a intervalos regulares con el fin de asegurarse de que son válidos y eficaces en situaciones adversas.

A.18 Conformidad		
A.18.1 Cumplimiento con los requisitos legales y contractuales		
Objetivo: Evitar violaciones de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de los requisitos de seguridad.		
A.18.1.1	Identificación de la legislación aplicable y requisitos contractuales	La empresa deberá mantenerse informada de los requisitos contractuales y leyes con el fin de cumplirlos
A.18.1.2	Derechos de propiedad intelectual	Se garantizará el uso de software del cual se tiene la propiedad intelectual.
A.18.1.3	Protección de los registros	Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, acceso no autorizado y la liberación no autorizada, de conformidad con los requisitos legales, reglamentarios, contractuales y de negocios.
A.18.1.4	Privacidad y protección de datos personales	La privacidad y protección de la información de identificación personal que se garantizará como se requiere en la LOPD y RGPD.
A.18.2 Revisiones de seguridad		
Objetivo: Garantizar que la seguridad informática es implementada y operada de acuerdo con las políticas y procedimientos de la organización.		
A.18.2.1	Revisión independiente de seguridad de la información	Siempre y cuando sea posible las revisiones serán llevadas a cabo por profesionales independientes a la empresa.
A.18.2.2	Conformidad con las políticas y normas de seguridad	Los responsables del cumplimiento deberán determinar la forma de revisar cómo se cumplen las políticas y normas de seguridad. En el caso de incumplimiento, se tomarán medidas correctivas.
A.18.2.3	Revisión de cumplimiento técnico	Los sistemas de información se revisarán periódicamente para identificar fallos en las actualizaciones y corregir fallos antes que supongan un problema.

7.- CONCLUSIONES

Indudablemente, las tecnologías han supuesto un gran impacto en todo los sectores empresariales y en todos los tipos de empresas. El sector turístico y en concreto, los establecimientos hoteleros, no son ninguna excepción.

Es por ello, que pensar en hoteles, pequeñas y medianas empresas (PYMES)e informatización, no supondría ninguna novedad pero añadir a este contexto el concepto de seguridad, le da una visión especial que es la que me gustaría poder transmitir en el desarrollo de este trabajo.

Para ello, inicialmente y tal como se expone en la introducción pensamos que a través de la realización del trabajo se ha logrado la consecución del objetivo principal del mismo: definir una propuesta de seguridad basada en la ISO 27001 para una PYME hotelera, y se ha demostrado que la capacidad de defensa de una empresa reside más en la concienciación y una buena definición de políticas de seguridad que en caros dispositivos. Por lo que no hace falta ser una multinacional para poder llevar a cabo medidas de seguridad eficientes, es más, es un riesgo que ninguna empresa se puede permitir.

En cuanto a los objetivos secundarios que nos habíamos fijado, nos ha permitido adquirir una base conceptual importante, se ha podido lograr una primera visión cercana a la situación real tanto del entorno de las Pymes como del sector turístico a pesar de la naturaleza perecedera de los datos debido al constante cambio y evolución sobretodo del contexto económico-social y tecnológico que pueden propiciar un cambio total de paradigma, en cualquier momento. Aún así el desempeño ha sido positivo.

Además, a través del análisis de los servicios de tecnología más frecuentes en los hoteles, hemos llegado a un mejor conocimiento de este sector. A ello le añadimos, el estudio de los ataques informáticos más frecuentes que se han registrado en el sector hotelero.

Antes de acabar, por la parte que le corresponde a las ISO se ha pretendido un acercamiento hacia ellas y evidenciar la necesidad de su aplicación para hacer de la empresa una organización lo más fiable y segura posible. a su vez abrir una línea de futuro para un posible trabajo sobre la integración de las ideas de estas ISO en un plan de negocio con el objetivo de evaluar la viabilidad económica de una empresa integrando las máximas medidas de seguridad posibles desde el momento de su creación.

Este hecho abre unas líneas de trabajo futuro interesantes, que podrían centrarse en trazar una evolución histórica de la seguridad en las pymes del sector hotelero a través de los diferentes contextos que atraviesan cada uno de los factores de influencia: Pymes, turismo, hoteles, tecnología, seguridad informática y normativa.

Llegados a este punto podemos decir que, las tecnologías han modificado el modo en que las empresas- en este caso- los hoteles- se relacionan con sus clientes y tras haber realizado este trabajo, no cabe ninguna duda que la tecnología es imprescindible para que el sector avance de una forma dinámica e innovadora, pero siempre teniendo en cuenta que se deben cerrar las puertas que nos abre tras usarlas porque podrían llegar a convertir a nuestra mejor aliada en la actualidad en nuestra peor enemiga.

Finalmente, y para acabar, destacar el viraje del trabajo desde la idea inicial de un plan de asignación de niveles de seguridad a las Pyme dependiendo de sus recursos a lo que finalmente se ha convertido. Esto ha sido debido a las concreciones y cambios experimentados tras los primeros estudios sobre las diversas temáticas y la orientación del tutor. A pesar de las dificultades sufridas por la falta de conocimientos iniciales en el sector hotelero, la legislación de las PYME y el correcto uso de las ISO este trabajo ha sido llevado a cabo con la mayor de las pasiones.

BIBLIOGRAFIA

1. **DÍAS, C. (2016). Diferencias entre micro, pequeña y mediana empresa**. Retrieved 3 September 2020, from https://cincodias.elpais.com/cincodias/2016/08/02/pyme/1470120203_791862.html

2. **Empresas pequeñas, medianas y grandes: ¿cómo se diferencian?** - Think Big Empresas. (2019). Retrieved 3 September 2020, from https://empresas.blogthinkbig.com/

3. **Ingresos por habitación disponible (RevPAR)** Nacional y desglose por categorías(2056). (2020). Retrieved 3 September 2020, from https://www.ine.es/jaxiT3/Datos.htm?t=2056#!tabs-tabla

4. **Clasificación de los hoteles según sus estrellas**. (2019). Retrieved 3 September 2020, from https://lugaresyhoteles.es/clasificacion-hoteles-por-estrellas/

5. **Tecnología y redes en hoteles de 3 y 4 estrellas**(2020). Retrieved 6 September 2020, from https://www.ithotelero.com/wp-content/uploads/2014/12/ESTUDIO-CISCO-ITH-Tecnolog%C3%ADa-y-redes-en-hoteles-de-3-y-4-estrellas-espa%C3%B1oles.pdf

6. (2020). **Retrieved 3 September 2020**, https://www.consumoresponde.es/sites/default/files/articulos/Requisitos%20m%C3%ADnimos%20espec%C3%ADficos%20para%20Hostales.pdf

7. **Coca, S. (2020). Seguridad de redes para proteger la wifi de un hotel »** EL BLOG DE ASHOTEL. Retrieved 3 September 2020, from https://blog.ashotel.es/2017/10/02/seguridad-de-redes-para-proteger-el-wifi-de-un-hotel/

8. **Orsi, R. (2018). Wi-Fi Hacking at the Hotel Pool** | Secplicity - Security Simplified. Retrieved 3 September 2020, from https://www.secplicity.org/2018/03/02/wi-fi-hacking-hotel-pool/

9. **Ciberseguridad en hoteles: el elemento clave del que no te puedes olvidar** - ITH. (2020). Retrieved 3 September 2020, from https://www.ithotelero.com/noticias/ciberseguridad-en-hoteles-el-elemento-clave-del-que-no-te-puedes-olvidar/

10. **Cybersecurity at Hotels: 6 Threats For Hotels to Manage**. (2017). Retrieved 3 September 2020, from https://www.socialtables.com/blog/hospitality/cyber-security-hotels/

11. **Valle, M., & Valle, M. (2017). Un ataque de ransomware encierra en sus habitaciones a los clientes de un hotel** -Globb Security. Retrieved 3 September 2020, from https://globbsecurity.com/ataque-ransomware-encierra-habitaciones-los-clientes-hotel-40551/

12. **RevengeHotels: cibercrimen dirigido a recepciones de hotel en todo el mundo**. (2019). Retrieved 3 September 2020, from https://securelist.lat/revengehotels/89842/

13. **¿Qué es el spear phishing?. (2018). Retrieved 3** September 2020, from https://www.kaspersky.es/resource-center/definitions/spear-phishing

14. **¿Qué es el ransomware?. (2020). Retrieved 3 September 2020,** from https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware

15. **Un ransomware bloquea las habitaciones de hoteles pidiendo un rescate. (2017)**. Retrieved 3 September 2020, from https://www.adslzone.net/2017/01/29/ransomware-bloquea-las-habitaciones-hoteles-pidiendo-rescate/

16. **Organización Internacional de Normalización**.(2013).ISO 27001

17. **Real Academia Española. (2020).** Retrieved from https://www.rae.es/

18. **¿Qué son los ataques DDoS?.** (2018). Retrieved 3 September 2020, from https://latam.kaspersky.com/resource-center/threats/ddos-attacks

19. **SC Media UK. (2020).** Retrieved 3 September 2020, from https://insight.scmagazineuk.com/

20. **Twitter. (2020).** Retrieved 3 September 2020, from https://twitter.com/pbump/status/826878966908776448

21. **Kumar, M. (2020). Ransomware Hijacks Hotel Smart Keys to Lock Guests Out of their Rooms.** Retrieved 3 September 2020, from https://thehackernews.com/2017/01/ransomware-hotel-smart-lock.html

22. **(2020). Retrieved 3 September 2020**, from https://docs.broadcom.com/doc/attacks-on-point-of-sale-systems-en

23. **Marriott se enfrenta a 110 M € de multa por el hackeo de Starwood** | Hoteles y Alojamientos. (2020). Retrieved 3 September 2020, from https://www.hosteltur.com/129898_marriott-se-enfrenta-a-110-m-de-multa-por-el-hackeo-de-starwood.html

24. **Marriott recibe una multa de 110 millones por el robo de datos de clientes. (2019).** Retrieved 3 September 2020 https://elpais.com/economia/2019/07/10/actualidad/1562756692_805212.html

25. **Los hackers se han vuelto tan sofisticados que solo en la última década han robado casi 4.000 millones de datos**: estos son los hackeos más graves de los últimos 10 años. (2019). Retrieved 3 September 2020, from https://www.businessinsider.es/10-mayores-hackeos-datos-ultima-decada-524509

26. **DarkHotel: una campaña de espionaje en hoteles de lujo asiáticos. (2014).** Retrieved 3 September 2020, from https://www.kaspersky.es/blog/darkhotel-espionaje-en-hoteles-de-lujo-asiaticos/4809/

27. **(2020). Retrieved 3 September 2020**, from https://www.dbcybertech.com/pdf/Marriot-Breach-White-Paper.pdf

28. **Black SEO. (2020). Retrieved 3 September 2020,** from https://encyclopedia.kaspersky.com/glossary/black-seo/

29. **Professional, P. (2020). Protect virtual home tours against cyber crime** - Property Professional. Retrieved 3 September 2020, from https://propertyprofessional.co.za/2020/07/23/protect-virtual-home-tours-against-cybercrime/

30. **(2020). Retrieved 3 September 2020**, from https://eu.usatoday.com/story/tech/2019/11/27/protect-your-data-while-charging-phone-at-airport/4319388002/

31. **FM, Y. (2019). Chromecast: qué es, cómo funciona y qué se puede hacer con él.** Retrieved 3 September 2020, from https://www.xataka.com/basics/chromecast-que-como-funciona-que-se-puede-hacer

32. **Chromecast Hacking con Metasploit y Kali Linux.** (2020). Retrieved 3 September 2020, from https://www.elladodelmal.com/2018/10/chromecast-hacking-con-metasploit-y.html

33. **Cómo un español burló la seguridad de un hotel de lujo y logró controlar todas sus habitaciones** -Panda Security Mediacenter. (2014). Retrieved 3 September 2020, from https://www.pandasecurity.com/spain/mediacenter/noticias/hackeo-hotel-china/

34. **Marketing, N. (2019). Unlocking Mobile App Vulnerabilities in Hotel Room Keys - NowSecure**. Retrieved 3 September 2020, from https://www.nowsecure.com/blog/2019/10/23/unlocking-mobile-app-vulnerabilities-in-hotel-room-keys/

35. **Economic Impact | World Travel & Tourism Council (WTTC) . (2020)**. Retrieved 3 September 2020, from https://wttc.org/Research/Economic-Impact

36. **Los hoteles españoles baten récords de plazas y de empleo en julio** | Hoteles y Alojamientos. (2020). Retrieved 3 September 2020, from https://www.hosteltur.com/130826_record-de-plazas-hoteleras-y-de-empleo-en-julio.html

37. **Omni Hotels & Resorts Hit by Point-of-Sale Malware - Noticias de seguridad** . Trend Micro es. (2016, 14 junio). www.trendmicro.com. https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/omni-hotels-resorts-hit-by-point-of-sale-malware

38. **"Webinar Ciberseguidad: riesgos y estrategias en el sector hotelero"**. Youtube [Consulta: 3 de septiembre de 2020]

39. **ISO 27001 - Software ISO 27001 de Sistemas de Gestión**. (2020). Retrieved from https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

40. **ISO 27001 - Seguridad de la información: norma ISO IEC 27001/27002**. (2019). Retrieved from https://www.normas-iso.com/iso-27001/

41. **Ciberseguridad Normas ISO(2020).** Retrieved from https://www.scprogress.com/NOTICIAS/CyberNoticia47-20170824.pdf

42. **ISO 27001 - Certificado ISO 27001 punto por punto** - Presupuesto Online. (2020). Retrieved 6 September 2020, from https://normaiso27001.es/

43. **Si necesitas teletrabajar sigue estos consejos de seguridad**. (2020, April 02). Retrieved from https://www.incibe.es/protege-tu-empresa/blog/si-necesitas-teletrabajar-sigue-estos-consejos-seguridad-0

44. **Bondades y riesgos del BYOD.** (2019, March 05). Retrieved from https://www.incibe.es/protege-tu-empresa/blog/bondades-y-riesgos-del-byod

45. **Dispositivos extraíbles en entornos industriales**: Amenazas y buenas prácticas. (2020, March 05). Retrieved from https://www.incibe-cert.es/blog/dispositivos-extraibles-entornos-industriales-amenazas-y-buenas-practicas

46. **MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información** (N.o 630-12-171-8). (2012). https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

47. **PERCEPCIÓN Y USO DE LA TECNOLOGÍA POR EL CLIENTE 4.0 EN EL SECTOR HOTELERO.** (2019). ITH.

48. **INFORME E-PYME** 2018. (2018). ONTSI.

49. **Las MIPyMES en el mundo:elementos para una redefinición. (**20187). Debate económico,72-93. https://www.laes.org.mx/debate-economico-no-17/las-mypimes-en-el-mundo-elementos-para-una-redefinicion/

50. **Mercado hoteleros 2019.** (2019). Tinsa.

51. **EL SISTEMA ESPAÑOL DE CLASIFICACIÓN.** (2010). CEHAT.

52. **Mercado Hotelero en España Destinos Vacacionales**. (2019). Christie & CO.

53. **GUIJARRO, M. (2009). Estudio de la literatura y modelos de negocio de la implantación de crm - modelo cliente céntrico - como enfoque estratégico condicionante de la ventaja competitiva en la pyme**: estudio empírico de la aplicación de un crm, en agencias de viajes (doctorado). UPV.

54. **SPAIN 2020 ANNUAL RESEARCH**: KEY HIGHLIGHTS. (2020). WTTC.

55. **CÁMPORA, E. (2013). Estudio del impacto de las TIC en el turismo: análisis de su influencia en los habitantes de la ciudad de Gandía durante la planificación de un viaje** (TFG). UPV.

56. **PYMES (2018). Recuperado de Enciclopedia Económica** (https://enciclopediaeconomica.com/pymes/).

57. **Guía del usuario sobre la definición del concepto de pyme**. (2016). UE.

58. **Retrato de la PYME. DIRCE a 1 de enero de 2019**. (Febrero 2020) Dirección General de Industria y de la Pequeña y Mediana Empresa www.ipyme.org

59. **Obligaciones de los empresarios en materia de seguridad social : Astac** (2020). Retrieved from http://www.astac.info/obligaciones-de-los-empresarios/.

60. **Martín-Nieto, T. (2017). Obligaciones de la pyme en materia de desempleo**. Retrieved from https://cincodias.elpais.com/cincodias/2017/09/29/pyme/1506698313_126260.html

61. **De La Cámara Delgado, M. (2015). GPS-PYMEs: Marco de Gestión de Proyectos para el desarrollo** Seguro en PYMEs (Doctorado). Universidad Politécnica de Madrid.

62. **Criteria 2020** - 2025. (2020). Hotelstars.

63. **Estudio sobre el empleo en el sector turístico español**. (2018). Exceltur.

64. **Balance sector turismo en España** 2019. (2019). Bankia.

65. **Pulgarín, R. (2014). Elaboración de un plan de implementación de la ISO**/IEC 27001:2013 (Master). Universitat Autònoma de Barcelona.

66. **CUERVO ALVAREZ, S. (2017). Implementación ISO 27001** (TFM).

67. **Lluch Mesquida, C. (2015). Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI)** según la norma ISO 27001.

68. **Valor Creativo**.(2017).Trabajo ISO 27001.

69. (**2012). Digital Lock-Picking: This Simple Arduino Hack Opens Millions of Hotel Keycard Doors**. Retrieved 3 September 2020, from https://null-byte.wonderhowto.com/news/digital-lock-picking-simple-arduino-hack-opens-millions-hotel-keycard-doors-0138312/

ANEXO 1:
Criterios de clasificación de HOTELSTARS

Area	No.	Criterion	Points	☆	☆☆	☆☆☆	☆☆ ☆☆	☆☆ ☆☆☆
I. General Hotel Info								
Cleanliness / Hygiene	1	Cleanliness and hygiene are prerequisites as basic conditions in all categories.[1]	-	M	M	M	M	M
Preservation condition	2	All mechanisms and equipment are functional and in faultless condition.	-	M	M	M	M	M
General impression	3	The general impression of the hotel is sufficient for _____ requirements.	-	simple[2]	medium[3]	elevated[4]	high[5]	highest[6]
Staff	4	All services must be provided by competent and identifiable staff.	-	M	M	M	M	M
	5	Bilingual staff	3		M	M	M	M
Car Park	6	Parking directly at the hotel	3					
	7	Parking possibilities for busses	3					
	8	Garage	5					
	9	Charging station for electric cars	10					
	10	Dedicated charging station for electric bicycles or other types of electric transport	3					
Others	11	Min. 50% of the rooms with balcony or terrace	5					
	12	Elevator[7]	10				M	M
Facilities for disabled persons[8]	13	Barrier-free accessibility Wheelchair or assistance	5					

1 In times of the COVID-19 crisis, special obligations may apply with regard to cleaning and hygiene measures. Compliance with legal requirements and/or national regulations in this respect may override certain HSU criteria until further notice.
2 In particular, furnishing and equipment are appropriate and maintained.
3 In particular, furnishing and equipment are maintained and harmonized.
4 In particular, furnishing and equipment are consistent in form and colour. The general impression is that of elevated comfort.
5 In particular, furnishing and equipment are high-quality and offer first-class comfort. The overall appearance is consistent in form, colour and materials.
6 In particular, furnishing and equipment are luxurious and offer highest comfort. The overall appearance is consistent in form, colour, and materials.
7 For hotels with more than three floors (incl. ground floor).

Area	No.	Criterion		Points	★	★★	★★★	★★★★	★★★★★
	14	Barrier-free accessibility Electronic wheelchair		10					
	15	Barrier-free accessibility Blind or visually impaired		5					
	16	Barrier-free accessibility Deaf or hearing impaired		5					
II. Reception and Services									
Reception area	17	Designated (designed and signalled) area or desk securing privacy		1	M	M	M	M	M
	18	Separate and designated reception area or desk securing privacy		3					
	19	Lounge suite[9] in the reception area		3			M		
	20	Lobby[9] with seats and beverage service		5				M	M
	21	Reception hall[9] with several seats and beverage service		10					
	22	Reception service, available for digital communication or phone calls 24 hours		1	M	M			
	23	10 hours staffed reception service, available for digital communication or phone calls 24 hours		7			M		
	24	16 hours staffed reception service, physically available for digital communication or phone calls 24 hours		10				M	
	25	24 hours staffed reception service, physically available for digital communication or phone calls 24 hours		15					M
	26	Self-check-in facility / service		3					
	27	Self-check-out facility / service		3					

8 According to national regulations.
9 Criteria 19 to 21 differ in size and sentience interpretation (from small to big, from just a seating corner to a representative hall).

Area	No.	Criterion		Points	☆	☆☆	☆☆☆	☆☆ ☆☆	☆☆ ☆☆
	28	Valet parking service		10					M
	29	Doorman (separate personnel)		15					
	30	Concierge / Guest relation manager (separate personnel)		15					M
	31	Page boys (separate personnel)		15					
	32	Luggage service on demand		5			M	M	
	33	Luggage service		10					M
	34	Secure left-luggage service for guests		5			M	M	M
Cleaning of rooms / change of laundry	35	Daily room cleaning[10]		1	M	M	M	M	M
	36	Daily change of towels on demand		1	M	M	M	M	M
	37	Change of bed linen at least once a week[10]		1	M	M	M		
	38	Change of bed linen at least twice a week[10]		3				M	M
	39	Daily change of bed linen on demand		3				M	M
Laundry and ironing service	40	Ironing service (return within 1 hour)		3					M
	41	Laundry and ironing service (return as agreed, laundry bag provided)		1			M		
	42	Chemical cleaning / dry cleaning or laundry and ironing service (delivery before 9 a.m., return as agreed – weekend excluded, laundry bag provided)		7				M	M
Payment	43	Cashless payment		1	M	M	M	M	M

10 With the option of opting-out.

Area	No.	Criterion		Points	☆	☆☆	☆☆☆	☆☆ ☆☆	☆☆ ☆☆
Miscellaneous	44	Umbrella at the reception or in the room		3			M	M	M
	45	Up-to-date media in the room (printed or digital)[11]		3					M
	46	Sewing service		3					M
	47	Sewing kit on demand		1		M	M	M	
	48	Sewing kit in the room		3					M
	49	Shoe polishing machine in the hotel		5				M[12]	M
	50	Shoe polishing service		5				M[12]	M
	51	Shoe polishing kit on demand		1		M	M	M	
	52	Shoe polishing kit in the room		3					M
	53	Shuttle or limousine service		5					M
	54	Offer of sanitary products on demand (at least toothbrush, toothpaste, shaving kit, bath / shower gel)		1	M	M	M	M	M
	55	Personalized greeting for each guest with flowers or a present in the room		5					M
	56	Accompanying the guest to the room on arrival		5					
	57	Turndown service[13] in the evening as an additional room check		7					M

11 Newspapers, smart TV, tablets etc.
12 Either a shoe polishing machine in the hotel (see no. 49) or a shoe polishing service (see no. 50) can be offered.
13 Also called “Second service”. Change of towels, removal of bedspread, emptying of waste paper basket, etc.

Area	No.	Criterion	Points	★	★★	★★★	★★★★	★★★★★
III. Rooms								
General Room Info	58	Size of rooms (incl. bathroom) ≥ 14m² [14]	10					
	59	Size of rooms (incl. bathroom) ≥ 18m² [14]	15					
	60	Size of rooms (incl. bathroom) ≥ 22m² [14]	20					
	61	Size of rooms (incl. bathroom) ≥ 30m² [14]	25					
	62	Number of suites[15]	3 per suite, max. 9					M (min. 2)
Sleeping comfort	63	Bed system with a modern and well-kept mattress of at least 13 cm[16]	1	M	M			
	64	Bed system consisting of an elastic system in combination with a modern and well-kept mattress with an overall height of at least 18 cm[16, 17]	5			M	M	M
	65	Bed system consisting of an elastic system in combination with a modern and well-kept mattress with an overall height of at least 22 cm[16, 17]	7					
	66	Ergonomically adjustable bed system on demand	3					
Bed width[18]	67.1	Single beds min. width of 0.80m[19]	1					
	67.2	Single beds min. width of 0.90m[19]	5					M
	67.3	Single beds min. width of 1.00m[19]	10					

14 If the hotel has a limited number of rooms (max.15 %) that are below this size, the guest must be informed about this fact before the accommodation contract is made.
15 No “Junior suites“. Suites consist of at least two separate rooms; one of which is furnished as a bedroom and one as living room. The rooms do not need to be connected by a door; an opening is sufficient. Basically, a holiday flat in a dépendance is not considered a suite. In order to ensure that guests can make full use of the hotel services, suites must be situated in the hotel building.
16 The total height of the bed system is the sum of mattress and spring system (e.g. slatted frame).
17 The base of the system can be a box spring, a sprung slatted or any other equivalent system.
18 If a hotel has only single rooms or only double rooms, the number of points for the bed width will be doubled.
19 At the time of booking the guest must be informed, if there are two single beds in the room instead of a double bed or if a single bed is booked as a double bed. If the hotel has a limited number of beds (max.15 %) that are below this width, the guest must be informed about this fact before the accommodation contract is made.

Area	No.	Criterion		Points	☆	☆☆	☆☆☆	☆☆ ☆☆	☆☆ ☆☆
	67.4	Single beds min. width of 1.20m[19]		15					
	68.1	Double beds min. width of 1.40m[19]		1					
	68.2	Double beds min. width of 1.60m[19]		5					
	68.3	Double beds min. width of 1.80m[19]		10					M
	68.4	Double beds min. width of 2.00m[19]		15					
Bed length	69.1	Beds min. length of 1.90m		1					
	69.2	Beds min. length of 2.00m		5					M
	69.3	Beds min. length of 2.10m		10					
	69.4	Beds min. length of 2.20m		15					
	70	Crib on demand		1					
	71	Hygienic covers for mattresses[20] (“encasings”)		10					
	72	New acquisition of mattresses max. 5 years ago		10					
	73	Annual laundry or thorough cleaning of mattresses[21]		10					
	74	Allergy friendly bed linen and bed inlets available on demand[22]		3					
	75	Modern and well-kept blanket		1	M	M	M	M	M

20 A simple molleton mattress pad is not accepted. But a (chemo-thermally) washable, breathable, bedcover free from mites and their excrements, made of cotton or synthetic materials that is opened at the bottom side will fulfil this criterion.
21 This criterion is fulfilled, if there is no residual moistness, the mites are killed and their growth is eliminated.
22 Allergy-friendly should not be confused with allergy-free. Allergic pillows, blankets and bed linen should be confirmed by a certificate. The inlays and covers of the bed linen should also do without feathers and down.

Area	No.	Criterion		Points	☆	☆☆	☆☆☆	☆☆ ☆☆	☆☆ ☆☆
	76	Additional blanket on demand		1			M	M	M
	77	Modern and well-kept pillow		1	M	M	M	M	M
	78	Hygienic covers for pillows (“encasings”)		7					
	79	Annual pillow cleaning and / or renewal of pillows		1	M	M	M	M	M
	80	Additional usable, non-decorative pillow on demand		1			M	M	M
	81	Two usable, non-decorative pillows per person		5					M
	82	Pillow menu with a choice of different types		5				M	M
	83	Possibility to darken the room (e.g. curtain)		1	M	M	M	M	
	84	Possibility to completely darken the room (e.g. shutter or blackout curtain)		5					M
	85	Sheer curtain/screen/blinds or equivalent		3					
	86	Washable bedside carpet		3					
	87	Wake-up service		1	M	M	M	M	M
Room equipment	88	Adequate wardrobe or clothes niche		1	M	M	M	M	M
	89	Linen shelves		1		M	M	M	M
	90	Adequate number of hangers[23]		1	M	M	M		
	91	Adequate number of hangers of different types		3				M	M

23 Simple wired hangers do not fulfil this criterion.

Area	No.	Criterion		Points	☆	☆☆	☆☆☆	☆☆☆☆	☆☆☆☆☆
	92	Separate clothing hook		1	M	M	M	M	M
	93	1 seating accommodation		1	M	M			
	94	1 seating accommodation per person		3			M	M	M
	95	1 comfortable seating accommodation (upholstered chair/couch) with side table/tray		7				M	M
	96	1 additional comfortable upholstered chair or loveseat in double rooms or suites		7					M
	97	Table, desk top or similar work station		1	M	M			
	98	Table, desk top or similar work station with a free min. working space of 0.4 m^2, access to power socket and adequate lighting[24]		5			M	M	M
	99	Table, desk top or similar work station with a free min. working space of 0.6 m^2, access to power socket and adequate lighting[24]		7					
	100	Bedside table/tray		1			M	M	M
	101	Accessible power socket in the room[24]		1	M	M	M	M	M
	102	Additional accessible power socket next to the table/desk or desk top[24]		3					
	103	Additional accessible power socket next to the bed[24]		3			M	M	M
	104	Central light switch for the entire room light		3					
	105	Bedside light switch for the entire room light		3					
	106	Night light		1					

24 Power sockets must be available and not used by other stationary items.

Area	No.	Criterion		Points	☆	☆☆	☆☆☆	☆☆ ☆☆	☆☆ ☆☆☆
	107	Adequate room lighting		1	M	M	M	M	M
	108	Reading light next to the bed		3		M	M	M	M
	109	Dressing mirror		1			M	M	M
	110	Adequate place or rack to put the luggage/suitcase		5			M	M	M
	111	Wastepaper basket		1			M	M	M
Safekeeping	112	Safekeeping facilities (e.g. at the reception)		1	M	M			
	113	Central safe (e.g. at the reception)		3			M[25]	M[25]	M
	114	Safe in the room		5					M
	115	Safe with integrated power socket in the room		7					
Noise control / air conditioning	116	Adequate noise protection (windows)		7					
	117	Sound-absorbing doors or double doors		10					
	118	Rooms with centrally adjustable air conditioning		7					
	119	Rooms with individually adjustable air conditioning		10					
	120	Air conditioning in public guest areas (restaurant, lobby, entrance hall, breakfast room)		10					
	121	Harmonious atmosphere in public areas (light, smell, music, colour, etc.)		1					
Entertainment electronics	122	Audio or multimedia entertainment[26]		5			M	M	M

25 Or a safe in the room (see no. 114).
26 Entertainment options may include radio reception, separate players or streaming services.

Area	No.	Criterion		Points	☆	☆☆	☆☆☆	☆☆ ☆☆	☆☆ ☆☆
	123	Fixed electronic media in the bathroom		3					
	124	TV services with monitor in a size appropriate for the room with a remote function		1	M[27]	M[27]	M[27]	M	M
	125	Additional TV services with monitor in suites in a size appropriate for the room		3					
	126	International TV channels available		5				M	M
	127	International power adapter plug on demand		3				M	M
	128	Charging station (for multiple electronic devices) and/or different adapters on demand		1			M	M	M
Telecommunications	129	Device for internal and external communication on demand with an instruction manual (printed or digital)[28]		5			M	M	
	130	Device for internal and external communication in the room with a bilingual instruction manual (printed or digital)		10					M
	131	WIFI internet access in the public areas and in the rooms		1	M	M	M	M	M
	132	Secure internet connection (LAN, VPN or equivalent)		5					
	133	Private and secure printing option on demand		1				M	M
	134	Internet device in the room on demand		1					M
Miscellaneous	135	Guest directory (printed or digital)[29]		1	M	M			
	136	Bilingual guest directory (printed or digital)		5			M	M	M
	137	Regional information material available (printed or digital)		1	M	M	M	M	M
	138	Writing utensils and note pad		1			M	M	M

27 For testing purposes at national level, deviations may occur in Lithuania and the Czech Republic.
28 The guest must be informed about this offer during the check-in; a display, etc. is accepted.
29 The guest directory includes at least the breakfast time, the check-out time, and the opening hours of hotel facilities.

Area	No.	Criterion		Points	☆	☆☆	☆☆☆	☆☆ ☆☆	☆☆ ☆☆☆
	139	Correspondence folder		1					
	140	Trouser press		3					
	141	Iron and ironing board on demand or ironing room		1					
	142	Iron and ironing board in the room		3					
	143	Shoehorn in the room		1				M	M
	144	Door viewer		3					
	145	Additional locking mechanism at the room's door		1					
General Bathroom Info	146	Bathroom/Sanitary facilities ≥ 5m^2 [30]		10					
	147	Bathroom/Sanitary facilities ≥ 7,5m^2 [30]		15					
	148	100% of the rooms with shower/WC or bath tub/WC		1	M[31]	M[31]	M	M	M
	149	100% of the rooms with shower/WC or bath tub/WC and thereof 50% of the rooms with bath tub and separate shower cubicle		10					
	150	30% of the rooms with toilet separately		5					
	151	Shower with curtain or equivalent separations		1	M	M	M	M	M
	152	Shower with screen		5					
	153	Washbasin		1	M	M	M	M	M

30 If the hotel has a limited number of bathrooms (max. 15%) that are below this size, the guest must be informed about this fact before the accommodation contract is made.
31 If up to 15% of the hotel's rooms are not equipped with private showers/WC but offer shared showers/WC instead, the guest has to be informed of the fact that the room does not comply with the usual standard before the accommodation contract is made. This exception of a 15% deviation is not applicable to new buildings planned after 01.01.2020.

Area	No.	Criterion		Points	☆	☆☆	☆☆☆	☆☆ ☆☆	☆☆ ☆☆☆
	154	Twin wash basin in double rooms and suites		5					
	155	Washable bath mat		1			M	M	M
	156	Adequate lighting at the washbasin		1	M	M	M	M	M
	157	Permanent or removable anti-slip appliance in shower and bathtub		1					
	158	Safety handles		3					
	159	Mirror		1	M	M	M	M	M
	160	Accessible power socket near the mirror		1	M	M	M	M	M
	161	Vanity mirror		1					
	162	Flexible vanity mirror		3				M	M
	163	Lighted vanity mirror		1					
	164	Towel rails or towel hooks		1	M	M	M	M	M
	165	Heating option in the bathroom (e.g. heated towel rail)		5					M
	166	Storage surface		1	M	M	M		
	167	Large storage surface		3				M	M
	168	Toothbrush tumbler		1			M	M	M
	169	Soap or body wash at the wash basin		1	M	M	M	M	M
	170	Body wash or shower gel at the shower/bath tub		1		M	M	M	M

Area	No.	Criterion		Points	☆	☆☆	☆☆☆	☆☆ ☆☆	☆☆ ☆☆
	171	Shampoo[32]		1		M	M	M	M
	172	Additional cosmetic products (e.g. bath essence, shower cap, nail file, Q-tips, cotton wool pads, body lotion)		1 per item, max. 3				M	M
	173	Facial tissues		3			M	M	M
	174	Toilet paper in reserve		1	M	M	M	M	M
	175	1 hand towel per person		1		M	M	M	M
	176	1 bath towel per person		1	M	M	M	M	M
	177	Bathrobe on demand		3				M	
	178	Bathrobe		5					M
	179	Slippers on demand		1				M	
	180	Slippers		3					M
	181	Hairdryer on demand		1					
	182	Hairdryer		3			M	M	M
	183	Stool in the bathroom on demand		3					M
	184	Bathroom scales		1					
	185	Waste bin		1	M	M	M	M	M

32 This criterion is considered as fulfilled, if the bath essence or shower gel is suitable as shampoo as well, and this is indicated (on bottle or dispenser).

Area	No.	Criterion		Points	☆	☆☆	☆☆☆	☆☆ ☆☆	☆☆ ☆☆
IV. Gastronomy									
Beverages	186	Beverage offer in the hotel		1	M	M	M	M	M
	187	Beverage offer in the room		3			M	M	M
	188	Fridge in the room[33]		3					
	189	Minibar (with drinks and snacks)		5				M[34]	M
	190	Maxibar		3					
	191	16 hours beverages via room service		10				M[35]	
	192	24 hours beverages via room service		15					M
	193	Water boiler for tea / coffee together with accessories in the room		3					
	194	Coffee machine with accessories in the room		5					
Bar	195	Serviced bar or lounge area[36] (open at least 5 days per week)		7				M	
	196	Serviced bar or lounge area[36] (open 7 days per week)		10					M
Breakfast	197	Breakfast area		1	M	M	M	M	M
	198	Extended breakfast[37]		1	M				
	199	Breakfast buffet or equivalent breakfast menu card[38]		5		M	M		

33 Or Minibar (see no. 189)
34 Or Maxibar (see no. 190) or 16 hours beverages via room service (see no. 191).
35 Or Minibar (see no. 189) or Maxibar (see no. 190).
36 A beverage menu card must be available (printed or digital).
37 An extended breakfast includes at least one hot beverage (e.g. coffee or tea), a fruit juice, selection of fruits or fruit salad, a choice of bread and rolls with butter, jam, cold cuts and cheese.
38 Self-service offer with at least the same choice of products as in the extended breakfast with an egg or an egg-plate and cereals.

Area	No.	Criterion		Points	☆	☆☆	☆☆☆	☆☆ ☆☆	☆☆ ☆☆
	200	Breakfast buffet with service or equivalent breakfast menu card		10				M	M
	201	Breakfast menu card via room service		5					M
Food	202	Allergen friendly products (gluten-free, lactose-free etc.)		3					
	203	Regional dishes[39]		5					
	204	16 hours food offer via room service		10				M	
	205	24 hours food offer via room service		15					M
	206	Restaurant[40]		5 each, max. 10	M	M	M		
	207	Restaurant[40] open 5 days per week		7 each, max. 14				M	
	208	Restaurant[40] open 7 days per week		10 each, max. 20					M
V. Event Facilities (MICE)									
Banquet options	209	Banquet options for at least 50 people[41]		1					
	210	Banquet options for at least 100 people[41]		3					
	211	Banquet options for at least 250 people[41]		5					
Conference rooms	212	Designated co-working spaces / group working rooms		10					
	213	Conference room(s) of at least 100 m^2, ceiling height of at least 2.75 m[42]		10					

39 The food offer features a significant part of regional / national specialities. The majority of used products is from the region.
40 Each of them with a different concept, choice of food and location.
41 The restaurant area is not included.

Area	No.	Criterion		Points	☆	☆☆	☆☆☆	☆☆ ☆☆	☆☆ ☆☆☆
	214	Conference service[43] (separate department, separate available staff)		5					
	215	Daylight in the conference room and possibility to darken the room[43, 44]		1					
	216	Business centre (separate office and available staff)		5					
	217	Individually adjustable air conditioning of the conference rooms[43]		3					

VI. Leisure									
Sport	218	Adequate own recreation facilities onsite (indoor or outdoor)[45] (e.g. private garden, tennis court, beach or access to lake, golf course)		3 per facility, max. 9					
	219	Rental of sports equipment (e.g. skis, boats, bicycles)		3					
	220	Gym[46] with at least 4 different exercise machines (e.g. ergometer, dumb bell, machine for weight training, treadmill, rowing machine, stairmaster)		5					
Spa/Wellness[47]	221	Massages[48] (e.g. full body massage, lymph drainage, Shiatsu, foot reflexology)		3 per cabin, max. 9					
	222	Separate relaxation room[49]		3					
	223	Whirlpool or equivalent		3					

42 A conference room must have appropriate lighting (with artificial light 200lux), WIFI, a projector, a projection screen (appropriate to ceiling height and room size), a coat rack or locker and an adequate number of power sockets.
43 Acceptance only if criterion no. 213 is fulfilled.
44 Minimum criterion for every conference room.
45 Facilities are part of the hotel area and possible costs of use can be charged to the room.
46 The gym has a minimum size of 20m^2.
47 The spa area has to be accessible without crossing the conference or the restaurant area.
48 The cabins have a minimum size of 10m^2.
49 The relaxation room has a minimum size of 20m^2.

Area	No.	Criterion		Points	☆	☆☆	☆☆☆	☆☆ ☆☆	☆☆ ☆☆☆
	224	Sauna (with a minimum size of 6 seats)		3 per sauna type[50], max. 9					
	225	Beauty farm[48] with at least 4 different kinds of treatment (e.g. facial, manicure, pedicure, peeling and stress relaxation massage are offered)		5					
	226	Spa[48] with at least 4 different kinds of treatment (e.g. bath, Kneipp, hydrotherapy, moor, hammam, steambath)		10					
	227	Private spa cabin		5					
	228	Swimming pool (outdoor)[51] or swimming pond[52]		10					
	229	Swimming pool (indoor)[53]		10					
Children	230	In-house child care (for children younger than 3 years) for at least 3 hours on weekdays by skilled staff		10					
	231	In-house child care (for children older than 3 years) for at least 3 hours on weekdays by skilled staff		10					
	232	Children's area (playroom/ playground)		3					
	233	Baby equipment on demand (e.g. high chair, food warming equipment, changing mat, baby alarm)		3					
Others	234	Central sanitary facilities for hotel guests		3					
	235	Library		3					
	236	Host/animation programme		5					

50 Sauna types: "hot/dry" (e.g. Finnish sauna), "warm/slightly humid" (e.g. Tepidarium), or "warm/heavily humid" (e.g. steam room).
51 The outdoor swimming pool is heated and has a minimum size of 60m^2.
52 A swimming pond is a man-made, standing water body for swimming or bathing free of chemical water preparation.
53 The indoor swimming pool is heated and has a minimum size of 40m^2.

Area	No.	Criterion		Points	★	★★	★★★	★★★★	★★★★★
VII. Quality and Online Activities									
Quality Systems	237	Systematic complaint management system[54]		1			M	M	M
	238	Systematic analysis of guest reviews[55]		3				M	M
	239	Quality controls by mystery guesting[56]		5					
	240	Quality management system according EHQ[57] or equivalent		15					
Online Activities	241	Hotel own website[58] with updated information and realistic pictures together with the location of the hotel		1	M	M			
	242	Bilingual website[58] with updated information including the bed sizes and realistic pictures together with the location of the hotel		5			M	M	M
	243	Website with direct booking option		5					
	244	Website with guest reviews		3					
	245	Mobile responsive website or mobile application		5					
	246	Active invitation of departing/checked-out guests to write a review on a portal or on the website		5					
Others	247	Sustainability label / certificate[59]		20					

54 A systematic complaint management system includes structured complaint acceptance, evaluation, and response.
55 Active and systematic gathering and evaluation of guest opinions about the quality of the hotels services, analysis of weaknesses, and the realization of improvement.
56 For the Mystery guesting to be accepted the following aspects need to be fulfilled at least once during a classification period: by professional externals upon initiative and on the account of the hotel, analysed and documented. Hidden (internal) controls e.g. of the hotel chain or cooperation are accepted as equal.
57 European Hospitality Quality (EHQ) is the European Hospitality Quality scheme launched by HOTREC, the umbrella association of national trade associations representing hotels, restaurants, cafés, and similar establishments in Europe (cf. www.hotrec.eu). It serves as a reference model for national and regional quality schemes on European level.
58 Pictures have to show at least an exterior view, the public area and a room.
59 National decision on recognised labels and certificates.

ANEXO 2:
Amenazas según metodología Magerit

5. Amenazas

Se presenta a continuación un catálogo de amenazas posibles sobre los activos de un sistema de información. Para cada amenaza se presenta un cuadro como el siguiente:

[código] descripción sucinta de lo que puede pasar	
Tipos de activos: • que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** 1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

5.1. [N] Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

Origen:
Natural (accidental)

5.1.1. [N.1] Fuego

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema. **Ver:** EBIOS: 01- INCENDIO	

5.1.2. [N.2] Daños por agua

[N.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: inundaciones: posibilidad de que el agua acabe con recursos del sistema. **Ver:** EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA	

5.1.3. [N.*] Desastres naturales

[N.*] Desastres naturales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad

Descripción:

otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ...

Se excluyen desastres específicos tales como incendios (ver [N.1]) e inundaciones (ver [N.2]).

Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.

Ver:

EBIOS:

03 – CONTAMINACIÓN
04 - SINIESTRO MAYOR
06 - FENÓMENO CLIMÁTICO
07 - FENÓMENO SÍSMICO
08 - FENÓMENO DE ORIGEN VOLCÁNICO
09 - FENÓMENO METEOROLÓGICO
10 - INUNDACIÓN

5.2. [I] De origen industrial

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas puede darse de forma accidental o deliberada.

5.2.1. [I.1] Fuego

[I.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: incendio: posibilidad de que el fuego acabe con los recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 01- INCENDIO	

5.2.2. [I.2] Daños por agua

[I.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA	

5.2.3. [I.*] Desastres industriales

[I.*] Desastres industriales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ... Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 04 - SINIESTRO MAYOR	

5.2.4. [I.3] Contaminación mecánica

[I.3] Contaminación mecánica	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: vibraciones, polvo, suciedad, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 03 – CONTAMINACIÓN	

5.2.5. [I.4] Contaminación electromagnética

[I.4] Contaminación electromagnética	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: interferencias de radio, campos magnéticos, luz ultravioleta, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 14 - EMISIONES ELECTROMAGNÉTICAS 15- RADIACIONES TÉRMICAS 16 - IMPULSOS ELECTROMAGNÉTICOS	

5.2.6. [I.5] Avería de origen físico o lógico

[I.5] Avería de origen físico o lógico	
Tipos de activos: • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 28 - AVERÍA DEL HARDWARE 29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE	

5.2.7. [I.6] Corte del suministro eléctrico

[I.6] Corte del suministro eléctrico	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: cese de la alimentación de potencia **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA	

5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad

[I.7] Condiciones inadecuadas de temperatura y/o humedad	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 11- FALLAS EN LA CLIMATIZACIÓN	

5.2.9. [I.8] Fallo de servicios de comunicaciones

[I.8] Fallo de servicios de comunicaciones	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 13 - PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN	

5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales

[I.9] Interrupción de otros servicios y suministros esenciales	
Tipos de activos: • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, ... **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: no disponible	

5.2.11. [I.10] Degradación de los soportes de almacenamiento de la información

[I.10] Degradación de los soportes de almacenamiento de la información	
Tipos de activos: • [Media] soportes de información	**Dimensiones:** 1. [D] disponibilidad
Descripción: como consecuencia del paso del tiempo **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 28 - AVERÍA DEL HARDWARE 29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE	

5.2.12. [I.11] Emanaciones electromagnéticas

[I.11] Emanaciones electromagnéticas	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] media • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [C] confidencialidad

Descripción:

hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque.

Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.

Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés *"Transient Electromagnetic Pulse Standard").* Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de "*TEMPEST protection",* queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara.

No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.

Origen:

Entorno (accidental)
Humano (accidental o deliberado)

Ver:

EBIOS: 17 - INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS

5.3. [E] Errores y fallos no intencionados

Fallos no intencionales causados por las personas.

La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

Origen:
Humano (accidental)

Ver correlación de errores y amenazas.

5.3.1. [E.1] Errores de los usuarios

[E.1] Errores de los usuarios	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [Media] soportes de información	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc. **Ver:** EBIOS: 38 - ERROR DE USO	

5.3.2. [E.2] Errores del administrador

[E.2] Errores del administrador	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: equivocaciones de personas con responsabilidades de instalación y operación **Ver:** EBIOS: 38 - ERROR DE USO	

5.3.3. [E.3] Errores de monitorización *(log)*

[E.3] Errores de monitorización *(log)*	
Tipos de activos: • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad (trazabilidad)
Descripción: inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ... **Ver:** EBIOS: no disponible	

5.3.4. [E.4] Errores de configuración

[E.4] Errores de configuración	
Tipos de activos: • [D.conf] datos de configuración	**Dimensiones:** 1. [I] integridad
Descripción: introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. **Ver:** EBIOS: no disponible	

5.3.5. [E.7] Deficiencias en la organización

Obsoleta.

[E.7] Deficiencias en la organización	
Tipos de activos: • [P] personal	**Dimensiones:** 1. [D] disponibilidad
Descripción: cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc. **Ver:** EBIOS: no disponible	

5.3.6. [E.8] Difusión de software dañino

[E.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación inocente de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc. **Ver:** EBIOS: no disponible	

5.3.7. [E.9] Errores de [re-]encaminamiento

[E.9] Errores de [re-]encaminamiento	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera. **Ver:** EBIOS: no disponible	

5.3.8. [E.10] Errores de secuencia

[E.10] Errores de secuencia	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración accidental del orden de los mensajes transmitidos. **Ver:** EBIOS: no disponible	

5.3.9. [E.14] Escapes de información

Obsoleta: use E.19.

[E.14] Escapes de información	
Tipos de activos: •	**Dimensiones:** 1. [C] confidencialidad
Descripción: la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	

5.3.10. [E.15] Alteración accidental de la información

[E.15] Alteración accidental de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. **Ver:** EBIOS: no disponible	

5.3.11. [E.18] Destrucción de información

[E.18] Destrucción de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. **Ver:** EBIOS: no disponible	

5.3.12. [E.19] Fugas de información

[E.19] Fugas de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones • [P] personal (revelación)	**Dimensiones:** 1. [C] confidencialidad
Descripción: revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc. **Ver:** EBIOS: no disponible	

5.3.13. [E.20] Vulnerabilidades de los programas (software)

[E.20] Vulnerabilidades de los programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad 3. [C] confidencialidad
Descripción: defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. **Ver:** EBIOS: no disponible	

5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)

[E.21] Errores de mantenimiento / actualización de programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. **Ver:** EBIOS: 31 - FALLA DE FUNCIONAMIENTO DEL SOFTWARE 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes electrónicos • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. **Ver:** EBIOS: 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

5.3.16. [E.24] Caída del sistema por agotamiento de recursos

[E.24] Caída del sistema por agotamiento de recursos	
Tipos de activos: • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. **Ver:** EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO	

5.3.17. [E.25] Pérdida de equipos

[E.25] Robo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. **Ver:** EBIOS: 22 - RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS	

5.3.18. [E.28] Indisponibilidad del personal

[E.28] Indisponibilidad del personal	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [D] disponibilidad
Descripción: **a**usencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, ... **Ver:** EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL	

5.4. [A] Ataques intencionados

Fallos deliberados causados por las personas.

La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

Origen:
Humano (deliberado)

Ver correlación de errores y amenazas.

5.4.1. [A.3] Manipulación de los registros de actividad (log)

[A.4] Manipulación de los registros de actividad (log)	
Tipos de activos: • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad (trazabilidad)
Descripción: **Ver:** EBIOS: no disponible	

5.4.2. [A.4] Manipulación de la configuración

[A.4] Manipulación de la configuración	
Tipos de activos: • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [A] disponibilidad
Descripción: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. **Ver:** EBIOS: no disponible	

5.4.3. [A.5] Suplantación de la identidad del usuario

[A.5] Suplantación de la identidad del usuario	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [A] autenticidad 3. [I] integridad
Descripción: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. **Ver:** EBIOS: 40 - USURPACIÓN DE DERECHO	

5.4.4. [A.6] Abuso de privilegios de acceso

[A.6] Abuso de privilegios de acceso	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas. **Ver:** EBIOS: 39 - ABUSO DE DERECHO	

5.4.5. [A.7] Uso no previsto

[A.7] Uso no previsto	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [C] confidencialidad 3. [I] integridad
Descripción: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc. **Ver:** EBIOS: no disponible	

5.4.6. [A.8] Difusión de software dañino

[A.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación intencionada de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc. **Ver:** EBIOS: no disponible	

5.4.7. [A.9] [Re-]encaminamiento de mensajes

[A.9] [Re-]encaminamiento de mensajes	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe. **Ver:** EBIOS: no disponible	

5.4.8. [A.10] Alteración de secuencia

[A.10] Alteración de secuencia	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados. **Ver:** EBIOS: 36 - ALTERACIÓN DE DATOS	

5.4.9. [A.11] Acceso no autorizado

[A.11] Acceso no autorizado	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dim1nsiones:** 1. [C] confidencialidad 2. [I] integridad
Descripción: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. **Ver:** EBIOS: 33 - USO ILÍCITO DEL HARDWARE	

5.4.10. [A.12] Análisis de tráfico

[A.12] Análisis de tráfico	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”. **Ver:** EBIOS: no disponible	

5.4.11. [A.13] Repudio

[A.13] Repudio	
Tipos de activos: • [S] servicios • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad (trazabilidad)
Descripción: negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro. **Ver:** EBIOS: 41 - NEGACIÓN DE ACCIONES	

5.4.12. [A.14] Interceptación de información (escucha)

[A.14] Interceptación de información (escucha)	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada. **Ver:** EBIOS: 19 - ESCUCHA PASIVA	

5.4.13. [A.15] Modificación deliberada de la información

[A.15] Modificación deliberada de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. **Ver:** EBIOS: no disponible	

5.4.14. [A.18] Destrucción de información

[A.18] Destrucción de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. **Ver:** EBIOS: no disponible	

5.4.15. [A.19] Divulgación de información

[A.19] Revelación de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: revelación de información. **Ver:** EBIOS: 23 – DIVULGACIÓN 27 – GEOLOCALIZACIÓN 34 - COPIA ILEGAL DE SOFTWARE	

5.4.16. [A.22] Manipulación de programas

[A.22] Manipulación de programas	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. **Ver:** EBIOS: 26 - ALTERACIÓN DE PROGRAMAS	

5.4.17. [A.23] Manipulación de los equipos

[A.22] Manipulación de los equipos	
Tipos de activos: • [HW] equipos • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [C] confidencialidad 2. [D] disponibilidad
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. **Ver:** EBIOS: 25 - SABOTAJE DEL HARDWARE	

5.4.18. [A.24] Denegación de servicio

[A.24] Denegación de servicio	
Tipos de activos: • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. **Ver:** EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO	

5.4.19. [A.25] Robo

[A.25] Robo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 3. [D] disponibilidad 4. [C] confidencialidad
Descripción: la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. **Ver:** EBIOS: 20 - ROBO DE SOPORTES O DOCUMENTOS 21 - ROBO DE HARDWARE	

5.4.20. [A.26] Ataque destructivo

[A.26] Ataque destructivo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: vandalismo, terrorismo, acción militar, ... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal. **Ver:** EBIOS: 05 - DESTRUCCIÓN DE HARDWARE O DE SOPORTES	

5.4.21. [A.27] Ocupación enemiga

[A.27] Ocupación enemiga	
Tipos de activos: • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo. **Ver:** EBIOS: no disponible	

5.4.22. [A.28] Indisponibilidad del personal

[A.28] Indisponibilidad del personal	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [D] disponibilidad
Descripción: ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, ... **Ver:** EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL	

5.4.23. [A.29] Extorsión

[A.29] Extorsión	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido. **Ver:** EBIOS: no disponible	

5.4.24. [A.30] Ingeniería social (picaresca)

[A.30] Ingeniería social (picaresca)	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. **Ver:** EBIOS: no disponible	

5.5. Correlación de errores y ataques

Errores y amenazas constituyen frecuentemente las dos caras de la misma moneda: algo que le puede pasar a los activos sin animosidad o deliberadamente. Se pueden dar hasta tres combinaciones:

- amenazas que sólo pueden ser errores, nunca ataques deliberados
- amenazas que nunca son errores: siempre son ataques deliberados
- amenazas que pueden producirse tanto por error como deliberadamente

Para afrontar esta casuística, errores y amenazas se han numerado de tal manera que pueda establecerse este paralelismo. La siguiente tabla alinea errores con ataques mostrando cómo se correlacionan:

número	*error*	*ataque*
1	Errores de los usuarios	
2	Errores del administrador	
3	Errores de monitorización *(log)*	Manipulación de los registros de actividad
4	Errores de configuración	Manipulación de la configuración
5		Suplantación de la identidad del usuario
6		Abuso de privilegios de acceso
7	~~Deficiencias en la organización~~	Uso no previsto
8	Difusión de software dañino	Difusión de software dañino
9	Errores de [re-]encaminamiento	[Re-]encaminamiento de mensajes
10	Errores de secuencia	Alteración de secuencia
11		Acceso no autorizado
12		Análisis de tráfico
13		Repudio
14	~~Escapes de información~~	Interceptación de información (escucha)
15	Alteración accidental de la información	Modificación deliberada de la información
18	Destrucción de información	Destrucción de información
19	Fugas de información	Revelación de información
20	Vulnerabilidades de los programas (software)	
21	Errores de mantenimiento / actualización de programas (software)	
22		Manipulación de programas
23	Errores de mantenimiento / actualización de equipos (hardware)	Manipulación de los equipos
24	Caída del sistema por agotamiento de recursos	Denegación de servicio
25	Pérdida de equipos	Robo
26		Ataque destructivo
27		Ocupación enemiga
28	Indisponibilidad del personal	Indisponibilidad del personal
29		Extorsión
30		Ingeniería social (picaresca)