Ciberseguridad en el sector Turismo y Ocio

Guía de recomendaciones para las empresas

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa
GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO
SECRETARÍA DE ESTADO DE TURISMO
SEGITTUR
turismo e innovación

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 INTRODUCCIÓN

Hoy en día es indudable que la **transformación digital** se encuentra cada vez más inmersa en los procesos de negocio. Su adopción permite a las empresas disponer de mayores y mejores ventajas competitivas en el mercado, aumentando también su productividad y rentabilidad, mejoras que de otro modo no serían posibles.

Iniciativas como **España Digital 2025** **[REF - 1]** apoyan e impulsan este proceso de transformación digital dentro del país, como una de las palancas fundamentales para relanzar el crecimiento económico, la reducción de la desigualdad, el aumento de la productividad y el aprovechamiento de todas las oportunidades que brindan las nuevas tecnologías.

En este escenario la gestión de la **ciberseguridad** cobra un papel fundamental para que este proceso de trasformación no suponga un riesgo para las empresas, por lo que la presente guía tiene como principal objetivo **promover una transformación digital segura y con garantías dentro del sector del turismo y ocio**, tratando para ello los principales aspectos clave en ciberseguridad que afectan al sector dentro de dicha transformación.

Esta guía se dirige, por tanto, a empresas que ofrecen servicios en destinos turísticos y/o de ocio, como pueden ser empresas de alojamientos, restauración, actividades recreativas o culturales; así como a aquellas que facilitan al usuario hacer uso de dichos destinos, englobando aquí agencias de viajes o de alquiler de vehículos, entre otros. También se consideran a los proveedores de servicios tecnológicos para estas empresas como parte del ecosistema para la concienciación y aplicación de la ciberseguridad.

Dentro del objetivo marcado, y debido a la gran variedad de empresas pertenecientes a este sector, esta guía, realizada por INCIBE, en colaboración con SEGITTUR, se centra en las **microempresas, pymes y autónomos a nivel nacional**, excluyendo del presente estudio a las grandes empresas.

Para cumplir con el objetivo marcado la guía desarrolla, en primer lugar, una **caracterización de la ciberseguridad aplicada al sector**, detallando para ello la dependencia tecnológica y el perfil de ciberseguridad de las distintas empresas que integran el sector.

En segundo lugar, se analizan las **principales amenazas de ciberseguridad** a las que están expuestas las empresas que engloban el sector, siempre teniendo en cuenta el alcance establecido.

Por último, se abordan y detallan los **principales aspectos** a tener en cuenta **en materia de ciberseguridad dentro del sector**, destacando las distintas medidas necesarias para proteger la información que gestionan y transmitir de este modo una imagen positiva de la organización entre sus clientes y proveedores.

1.1. Glosario de términos

En el mundo de la ciberseguridad se emplean términos y acrónimos de perfil técnico que no se usan en el día a día, sobre todo en el caso de personas que no se dedican al ámbito de la ciberseguridad. Por este motivo, INCIBE pone a disposición de los usuarios un **glosario de términos** **[REF - 2]**, ayudando de este modo a todos los perfiles en la comprensión de esta guía.

2 CARACTERIZACIÓN DE LA CIBERSEGURIDAD APLICABLE AL SECTOR

En este apartado se pretende analizar, en primer lugar, la dependencia tecnológica de las distintas empresas del sector, teniendo en cuenta los principales aspectos a considerar, como son la categorización de las empresas implicadas y las diferentes soluciones que más comúnmente utilizan para prestar sus servicios.

En segundo lugar, se obtienen los diferentes perfiles de ciberseguridad de las empresas del sector, identificándolos como el nivel de riesgo al que se encuentran expuestas.

2.1. ¿Qué es la ciberseguridad?

El primer paso es conocer el término **ciberseguridad**, que si bien es un concepto bastante amplio, se puede definir en el contexto de esta guía, como la práctica de proteger nuestros sistemas de información y todo lo que engloban (redes de comunicación, dispositivos, aplicaciones, etc.) de posibles ataques malintencionados. Por lo general, a través de estos ciberataques se podría acceder, modificar o destruir información confidencial, extorsionar a los usuarios o llegar a interrumpir la continuidad del negocio.

Cada vez hay más dispositivos conectados y los ciberdelincuentes son más ingeniosos. Por todos estos motivos, podemos afirmar que la ciberseguridad es un factor fundamental en todas las empresas, ya sean pymes, autónomos o grandes corporaciones.

La ciberseguridad es un **proceso**, y como tal, los planes para abordarla deben actualizarse periódicamente, ya que las amenazas cambian y evolucionan constantemente. Además, es un factor diferenciador para la empresa, al generar confianza tanto en clientes como en proveedores.

Hoteles, restaurantes, locales de ocio, agencias de viajes, gimnasios, etc., conforman un importante tejido empresarial y de gran peso en la economía de nuestro país, en el que las nuevas tecnologías son la base para su desarrollo.

En el desarrollo de su actividad, las empresas gestionan una gran cantidad de información de los clientes: datos personales y bancarios necesarios para realizar reservas, compras, suscripciones a servicios, etc. Un incidente de seguridad podría poner en riesgo la confidencialidad de esta información, afectando no solo a la imagen y reputación de la empresa, sino que, además, podría tener consecuencias legales **[REF - 3]**.

Por ello, es esencial conocer medidas de seguridad que protejan la información de la organización, así como de los sistemas que la gestionan, y de esta forma, contribuir también a la generación de confianza en clientes y proveedores.

2.2. Dependencia tecnológica

El proceso de transformación digital conlleva un cambio tecnológico cada vez más dinámico y constante, donde cobran una especial relevancia las **tecnologías disruptivas**, como el IoT (*Internet of Things*), la inteligencia artificial, el análisis avanzado de datos (*big data*) o la robótica, todas ellas consideradas como la piedra angular de la digitalización.

Es por ello que el avance tecnológico es cada vez mayor, y la oferta de integración tecnológica para cada sector de negocio muy diversa, dependiendo de aspectos como el tamaño de la organización o los procesos que integre para ofrecer sus servicios.

Hablar de dependencia tecnológica en este sector aborda, por tanto, la identificación de, por un lado, los diferentes tipos de empresas que se engloban en él, caracterizadas por el servicio que ofrecen o la actividad que realizan, y por otro lado, las diferentes tecnologías utilizadas por cada uno de estos tipos de empresas, con el fin de poder ofrecer sus servicios.

2.2.1. Tipos de empresas del sector

Hoy en día existe una gran variedad de oferta turística y de ocio, lo que diversifica en gran medida los servicios ofrecidos por este sector. En cualquier caso, hay que considerar que el producto turístico está constituido por servicios, puesto que su prestación efectiva está vinculada a la interacción con el cliente.

A pesar de esta gran variedad de oferta, una primera clasificación del sector se puede determinar en función de la **naturaleza del servicio** que se proporciona, identificando si este se ofrece en un destino turístico y/o de ocio o, si por el contrario, facilita al usuario hacer uso de dichos destinos.

Empresas que ofrecen servicios en destinos turísticos	» Alojamientos* » Gastronomía o restauración » Actividades recreativas y oferta cultural*	» Hoteles, *campings*, casas rurales, apartamentos, etc. » Restaurantes, bares, etc. » Museos, cines, teatros, etc.
Empresas facilitadoras	» Agencias de viajes (físicas y online)* » Transporte* » Tour operadores** » Centrales de reservas**	» Mayoristas y minoristas » Alquiler de vehículos y otros

Tabla 1. Tipos de empresas y servicios del sector

* Estos servicios no son ofrecidos exclusivamente o en su mayoría por grandes empresas.
** Estos servicios son ofrecidos exclusivamente o en su mayoría por grandes empresas.

2

Nota: dentro de esta clasificación **hay que tomar en consideración solo a aquellos servicios y empresas que se encuentran dentro del alcance de la guía**, excluyendo de esta forma los tipos de empresas y servicios ofrecidos exclusivamente o en su mayoría por grandes empresas.

2.2.2. Soluciones tecnológicas utilizadas

Dentro del sector del turismo y ocio las empresas pueden utilizar un gran conjunto de soluciones tecnológicas, con el objetivo de conseguir una mayor ventaja competitiva, una mayor productividad y/o una mejor rentabilidad de sus procesos, avanzando a su vez en el proceso de transformación digital **[REF - 4]**.

A continuación, puede verse un listado con algunas de las soluciones más utilizadas habitualmente por el sector, clasificadas según el tipo de tecnología a la que pertenecen:

Cloud	» Soluciones para la gestión de clientes y recursos: CRM (Gestión de la Relación con Clientes), CRS (Sistema Central de Reservas), PMS (Sistema de Administración de Propiedades) y TPV (Terminal Punto de Venta). » Soluciones de comercio electrónico: web de venta online y pasarelas de pago. » Otras soluciones de alojamiento web y servicios de backup.
IoT *(Internet of Things)*	» Soluciones de comercio electrónico: aplicaciones de reserva online y pagos por móvil. » Soluciones para el control, conocimiento de afluencia y presentación de contenidos. » Soluciones para domotizar alojamientos u otros establecimientos turísticos. » Otras soluciones: pulseras inteligentes.
Big data	» Soluciones de gestión de recursos: RMS (Sistema de Gestión de Ingresos). » Soluciones para toma de decisiones estratégicas o marketing. » Soluciones para la mejora y/o personalización de la experiencia de usuario: motores de búsqueda avanzados, seguimiento, análisis de opiniones y materiales o sistemas de venta basados en realidad virtual.
Inteligencia artificial	» Soluciones de gestión de redes sociales (seguimiento y análisis). » Soluciones de soporte a la experiencia del viajero: asistentes virtuales y *chatbots*.
Infraestructura	» Soluciones para redes internas. » Soluciones para redes wifi (públicas/privadas). » Otras soluciones: portal cautivo.

Tabla 2. Soluciones tecnológicas más habituales del sector

2

Al listado anterior pueden incorporarse las principales tecnologías de ciberseguridad **[REF - 5]** que podrían ser utilizadas por las empresas del sector:

- Auditoría técnica.
- Seguridad en la nube.
- Seguridad en dispositivos móviles.
- Seguridad *e-commerce*.
- Protección *end-point*.
- Protección de las comunicaciones.
- Gestión de incidentes.
- Formación y concienciación.
- Cumplimiento legal.

2.2.3 Niveles de dependencia tecnológica

En función del tipo de empresa, caracterizada por el servicio que ofrece y/o actividad que realiza, y del tamaño de la misma, se puede determinar el conjunto de soluciones tecnológicas que serán necesarias para cumplir con su objetivo de negocio, y por tanto, su nivel de dependencia tecnológica.

De forma general, para cualquier sector de actividad se pueden aplicar los siguientes niveles de dependencia tecnológica:

- **Nivel bajo de dependencia tecnológica**: cuando el uso de soluciones tecnológicas y su grado de aplicación al negocio es el siguiente:
  - Se utilizan para realizar el trabajo administrativo.
  - Se utilizan aplicaciones dentro de la red de área local para mantenimiento de aplicativos con bases de datos y hojas de cálculo (clientes, finanzas, etc.).
  - Se utiliza Internet fundamentalmente para consulta y búsqueda de información.
  - Es posible que se utilice el correo electrónico como medio de comunicación con empresas proveedoras y con clientes, pero no es común que se disponga de servidor de correo.
  - Se puede disponer de una página web informativa (descarga de documentación, información de contacto, etc.), que generalmente se aloja externamente.

- Se utiliza la red de área local o wifi para compartir recursos (impresoras, discos, acceso a Internet, etc.), pudiendo disponer de un servidor de ficheros.

La siguiente figura muestra una infraestructura típica de este nivel de dependencia, generalmente **asociado a autónomos o microempresas**:

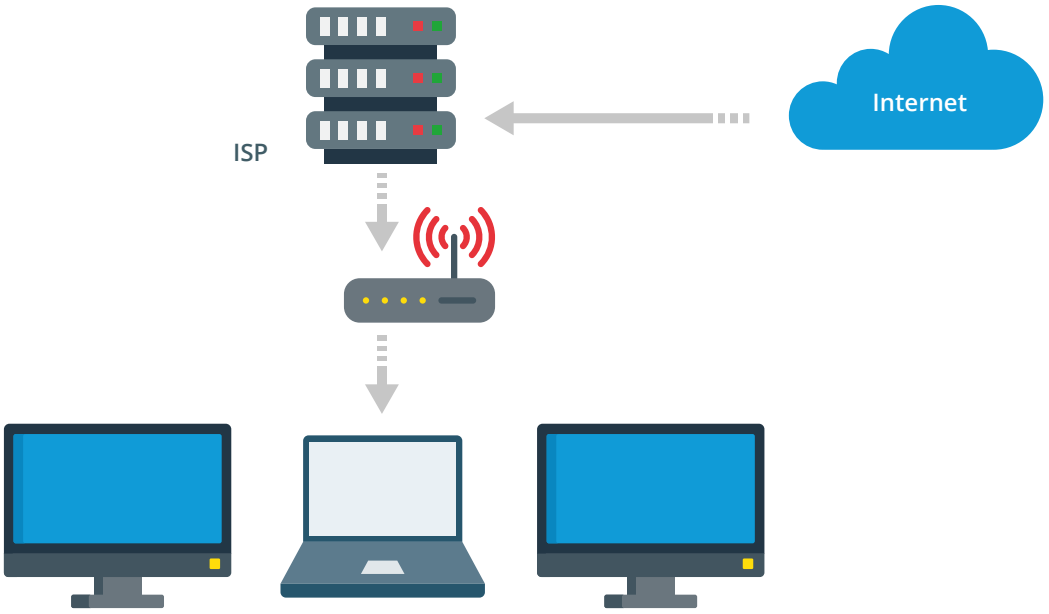


Figura 1. Infraestructura de nivel bajo de dependencia tecnológica

» **Nivel medio de dependencia tecnológica:** cuando el uso de soluciones tecnológicas y su grado de aplicación al negocio es el siguiente:

- Se utilizan herramientas colaborativas en red para gestión del negocio (procesos, RRHH, gestión de clientes, etc.).
- Se utiliza Internet para potenciar el negocio (*mailings*, publicidad, etc.) y para el cumplimiento de las obligaciones con la administración.
- Se dispone de servidores de correo electrónico que se administran localmente o se subcontrata el servicio.
- Se utiliza la red de área local para compartir recursos (aplicaciones, ficheros, etc.) con servidores propios.
- Se utiliza página web, que cambia con frecuencia de contenidos (noticias, boletines, RSS, catálogo de productos, etc.), y puede contener servicios interactivos (formularios, etc.).
- Es posible que se utilicen dispositivos portátiles para acceso remoto a la red corporativa.

2

La siguiente figura muestra una infraestructura típica de este nivel de dependencia, generalmente **asociado a pequeñas y medianas empresas**:

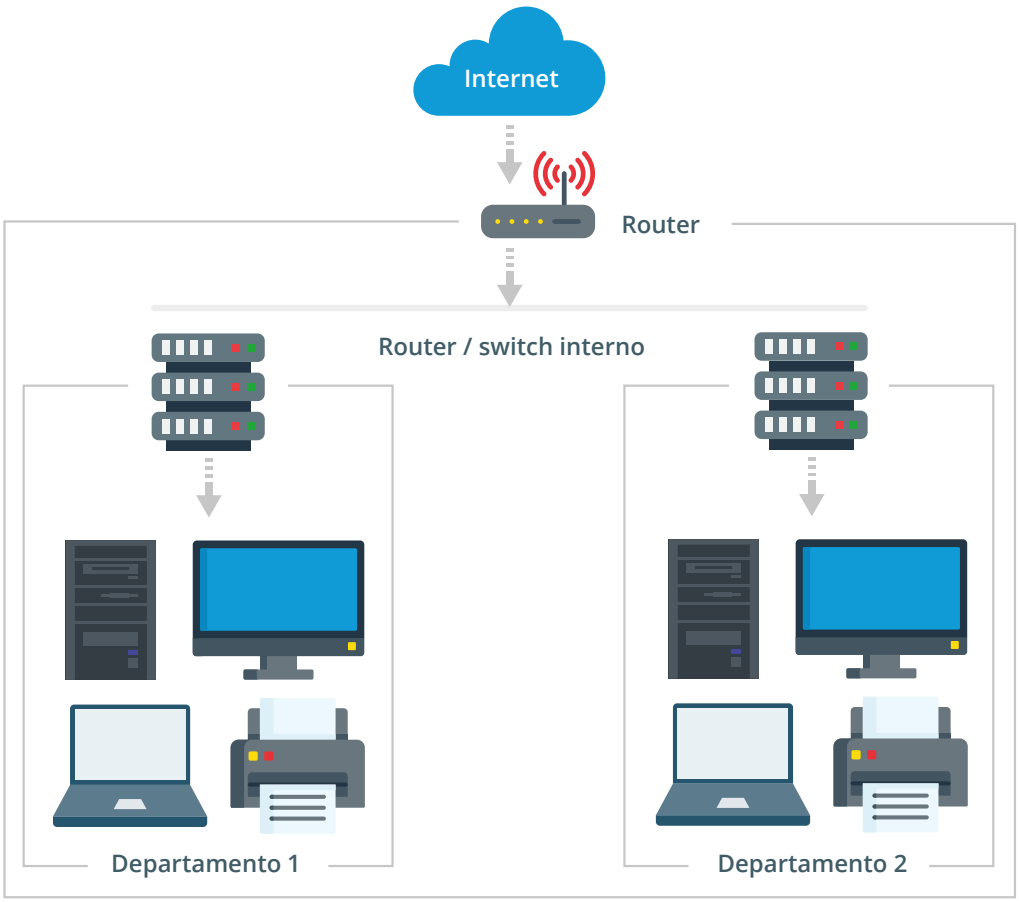


Figura 2. Infraestructura de nivel medio de dependencia tecnológica

» **Nivel alto de dependencia tecnológica:** cuando el uso de soluciones tecnológicas y su grado de aplicación al negocio es el siguiente:

- Se utiliza Internet u otras redes para el desarrollo del negocio (B2B, B2C, etc.).
- Es posible que se disponga de servicios/productos que se distribuyen y/o venden online.
- Se utiliza el intercambio electrónico para el desarrollo del negocio (contratación, facturación, etc.).
- Se dispone de una intranet (formación, aplicativos internos, etc.).
- La empresa forma redes particulares con sus proveedores y sus clientes (extranets).
- Se utilizan herramientas colaborativas de forma online.

2

La siguiente figura muestra una infraestructura típica de este nivel de dependencia, generalmente **asociado a medianas y grandes empresas***:

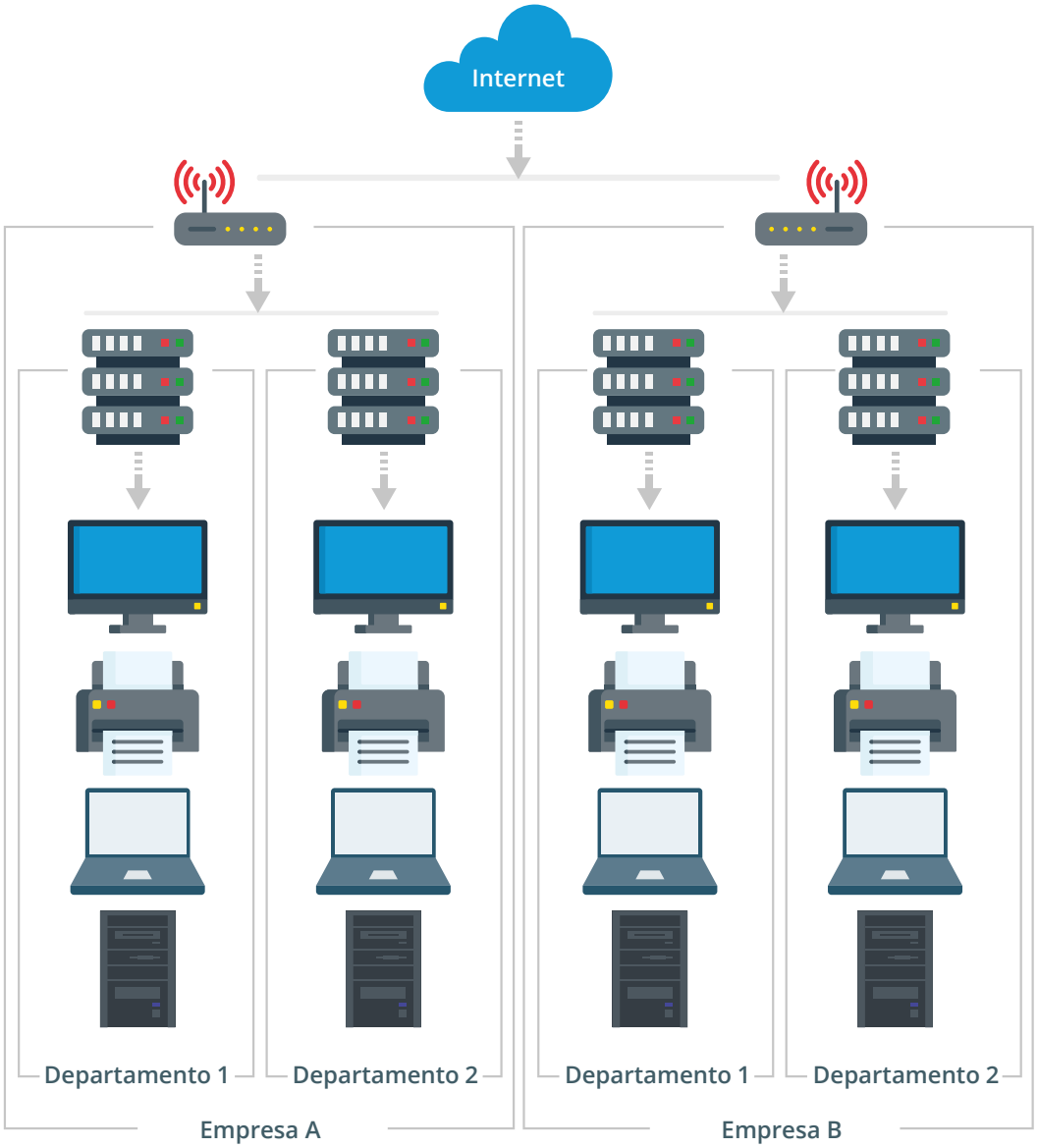


Figura 3. Infraestructura de nivel alto de dependencia tecnológica

* Hay que tener en cuenta que el alcance de la presente guía excluye a las grandes empresas.

A partir de la clasificación y definición anterior de los niveles de dependencia tecnológica, y de las soluciones tecnológicas aplicables al sector, en la siguiente tabla se establece una relación aproximada entre las **empresas del sector del turismo y ocio y su nivel de dependencia tecnológica**:

Nota: hay que tener en cuenta que el nivel asignado corresponde con el número máximo de soluciones que la empresa puede adoptar dentro de su categoría. Esto, a su vez, vendrá determinado por el **tamaño de la empresa**; por ejemplo, una microempresa que ofrezca alojamiento utilizará un número menor de soluciones tecnológicas que una mediana empresa que ofrezca el mismo servicio.

Alojamiento (hoteles familiares, *campings*, casas rurales, apartamentos, etc.)	Nivel de dependencia tecnológica Alto	» Soluciones cloud para la gestión de clientes y recursos: CRM, CRS, PMS o TPV. » Soluciones de comercio electrónico: web de venta online y pasarelas de pago. » Soluciones de gestión de recursos: RMS (Sistema de Gestión de Ingresos). » Soluciones para redes internas. » Soluciones para redes wifi públicas.
Gastronomía o restauración (restaurantes, bares, etc.)	Nivel de dependencia tecnológica Alto	» Soluciones cloud para la gestión de clientes y recursos: TPV. » Soluciones de comercio electrónico: web de venta online, pasarelas de pago, aplicaciones de reserva online, pagos por móvil. » Soluciones para redes wifi públicas.
Actividades recreativas y/o de oferta cultural*	Nivel de dependencia tecnológica Sin determinar	
Agencias de viajes físicas y online	Nivel de dependencia tecnológica Alto	» Soluciones cloud para la gestión de clientes y recursos: CRS y CRM. » Soluciones de gestión de recursos: RMS. » Soluciones de comercio electrónico: web de venta online y pasarelas de pago. » Soluciones para redes internas.
Alquiler de vehículos	Nivel de dependencia tecnológica Alto	» Soluciones cloud para la gestión de clientes y recursos: CRS. » Soluciones de comercio electrónico: web de venta online y pasarelas de pago.

Tabla 3. Niveles de dependencia tecnológica de las empresas del sector

* Las empresas que ofrecen este tipo de servicios pueden ser muy diversas, en cuanto al tipo de actividad y tamaño, por lo que las soluciones tecnológicas que utilizan dependerán de ambos factores, y por lo tanto, variará su nivel de dependencia tecnológica en función de los mismos.

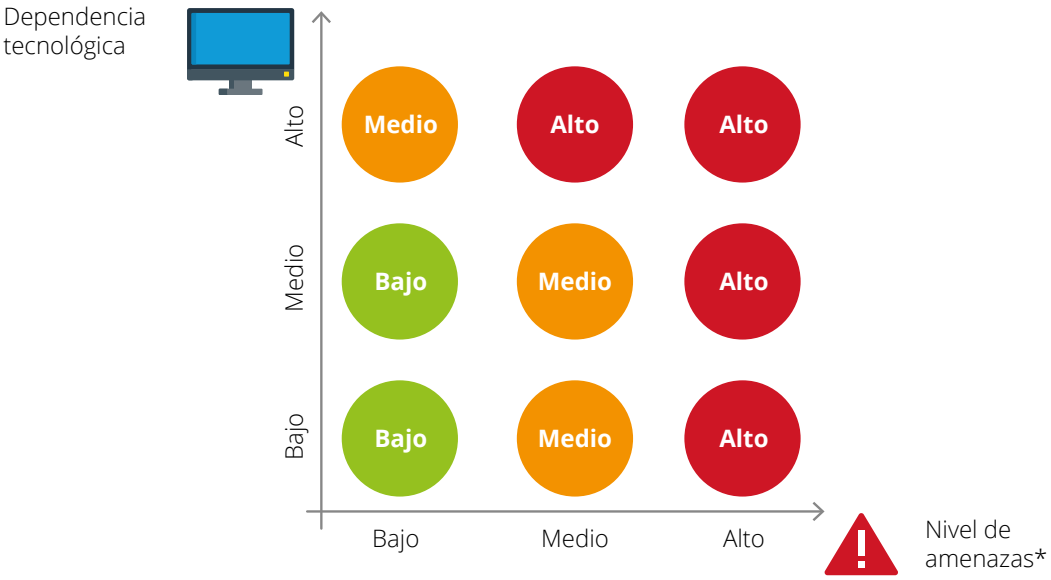
2.3. Perfiles de ciberseguridad

El perfil de ciberseguridad está determinado por el **nivel de riesgo al que se encuentra expuesta una organización**, pudiendo ser alto, medio o bajo. Estos valores, a su vez, están definidos por varios factores, entre los que se encuentran el nivel de dependencia tecnológica y el tipo de soluciones utilizadas, teniendo en cuenta que no todas las soluciones están expuestas al mismo número o tipo de amenazas de ciberseguridad.

La dependencia tecnológica viene derivada del conjunto de soluciones utilizadas en función de la actividad del negocio y el tamaño de la empresa, considerando la clasificación en autónomos, microempresas (1-9 empleados), pequeñas empresas (10-49 empleados), medianas empresas (50-249 empleados) y grandes empresas (>250 empleados).

Por tanto, se considera que una empresa tiene un perfil de ciberseguridad con **nivel de riesgo alto** cuando tiene, por ejemplo, una **alta dependencia tecnológica**, con **tecnologías expuestas a un número moderado de amenazas**, o una **dependencia tecnológica media**, con **tecnologías expuestas a un gran número de amenazas**.

En la siguiente tabla se puede ver la relación existente entre la dependencia tecnológica, el nivel de amenazas a las que están expuestas las soluciones (que depende de los tipos y número de amenazas), y el nivel riesgo en ciberseguridad de las organizaciones.



* En función del tipo y número de amenazas que afectan a la solución

Figura 4. Nivel de riesgo de los perfiles de ciberseguridad

No obstante, existen diversas herramientas y servicios en el mercado con el objetivo de que las empresas puedan evaluar su nivel de riesgo en ciberseguridad, y de esta forma, comenzar a mejorar su protección. Dentro de estos servicios INCIBE proporciona **la herramienta de autodiagnóstico** **[REF - 6]**, que ofrece un primer punto de partida para conocer el estado actual de ciberseguridad de la organización.

3 PRINCIPALES AMENAZAS DE CIBERSEGURIDAD EN EL SECTOR

Ser consciente de las amenazas y conocerlas a fondo es esencial para poder evitarlas, y así proteger nuestros sistemas e información **[REF - 7]**. Ciberataques de *ransomware* y *phishing* o contra la página web, fugas de información, uso de redes inalámbricas o acceso remoto a los sistemas, administración de perfiles en redes sociales o relaciones con proveedores tecnológicos, son solo algunas de las amenazas a las que constantemente están sometidas las empresas de este sector.

3.1. Amenazas a través de correo electrónico

Las amenazas más comunes que afectan a las empresas de turismo y ocio tienen su origen en el correo electrónico, que junto con la ingeniería social **[REF - 8]**, se convierten en un instrumento muy eficaz para que los ciberdelincuentes se lucren a través del fraude, la estafa y la extorsión.

En la actualidad, el fraude online es una de las ciberamenazas que más preocupa a las organizaciones. Los ciberdelincuentes utilizan la combinación de la ingeniería social y las herramientas tecnológicas para engañar tanto a empresarios como a empleados. Este tipo de estafas, por lo general, se realizan a través del correo electrónico y tienen principalmente una motivación económica para el ciberdelincuente.

Entre los casos más habituales se encuentra **la suplantación de identidad por correo electrónico**, utilizando la técnica de *e-mail spoofing* **[REF - 9]**. Mediante esta técnica los ciberdelincuentes envían correos con remitente falso para enviar *spam* **[REF - 10]**, difundir *malware* **[REF - 11]** o llevar a cabo ataques de *phishing* **[REF - 12]**, suplantando en este último caso la identidad de perfiles con capacidad de toma de decisiones en la empresa (CEO o CISO), proveedores, clientes, etc. La ingeniería social suele ser el aliado perfecto para que las víctimas no sospechen del engaño.

Entre los principales casos de fraude a través del correo en los que se utiliza la suplantación de identidad, cabe destacar:

- **El falso soporte técnico** **[REF - 13]**: se trata de un fraude donde el estafador se hace pasar por el servicio informático de la compañía con el pretexto de solucionar ciertos problemas técnicos en el equipo. El objetivo es principalmente obtener acceso al ordenador de la víctima, para así conseguir información confidencial de la empresa. También es muy habitual la variante del **falso soporte de Microsoft** **[REF - 14]**.

3

» **El fraude del CEO** **[REF - 15]**: consiste en engañar a un empleado con capacidad para hacer movimientos bancarios o acceder a datos de cuentas de la empresa. Este recibe un correo, suplantando la identidad de su jefe, ya sea el CEO, presidente o director de la organización en cuestión, donde se le pide ayuda para que realice una operación financiera confidencial y urgente. El objetivo es transferir fondos de la empresa a la cuenta del ciberdelincuente. Este fraude tiene diversas variantes **[REF - 16],** si bien el fin siempre es el mismo.

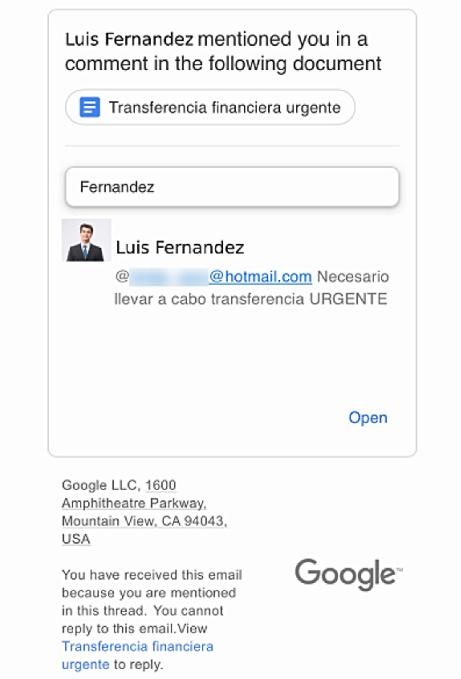


Figura 5. Fraude del CEO a través de Google Drive

» **El fraude de RR. HH.** **[REF - 17]:** esta vez el correo va dirigido al personal de Recursos Humanos de la empresa. En este correo el ciberdelincuente suplanta la identidad de un empleado, solicitando un cambio de cuenta para el ingreso de su nómina. Al igual que el fraude del CEO, el objetivo es que la organización transfiera dinero a la cuenta del estafador.

Figura 6. Correo ejemplo de suplantación del empleado

3

Otra de las amenazas más comunes a través del correo electrónico es la **extorsión**, en la que el ciberdelincuente chantajea a la víctima, indicándola que tiene en su poder información sensible sobre esta. Existen distintas formas de extorsionar a una empresa:

» **Campañas de distribución de *ransomware*:** entre las extorsiones más extendidas en el ámbito empresarial se encuentra el caso particular del *ransomware* **[REF - 18]**.

La extorsión se realiza a través de este tipo de *malware*, que se introduce en los equipos de las empresas, principalmente a través de un señuelo enviado por correo electrónico. En estos correos se insta a la víctima a descargar y ejecutar archivos con código malicioso que infectarán el equipo. Una vez infectado, el funcionamiento del *ransomware* es cifrar los archivos del dispositivo para que ya no sean accesibles para el usuario. Normalmente, se propaga a través de la red de la empresa, infectando así todos los equipos de la organización.

A cambio de devolver el acceso a esta información a la empresa, los ciberdelincuentes piden una compensación económica, chantaje al que nunca se debe acceder. Nadie asegura que con este pago la información secuestrada quede liberada, y además, se contribuye a aumentar la incidencia de este tipo de ciberdelincuencia.

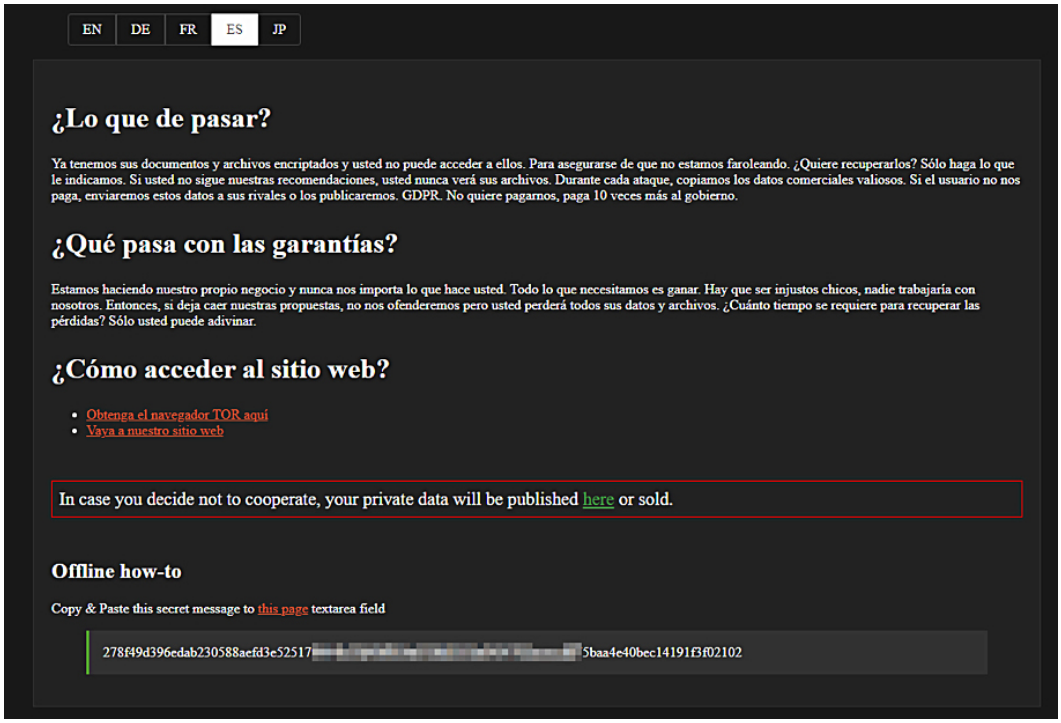


Figura 7. Nota de rescate de ransomware

» **Campañas de sextorsión** **[REF - 19]:** este tipo de campañas tienen muchas variantes, ya que los ciberdelincuentes van cambiando ligeramente el contenido del mensaje. El objetivo del correo es extorsionar a los destinatarios con un supuesto vídeo de contenido sexual, que se enviará a la lista de contactos de la víctima si esta no accede a ingresar la cantidad de dinero, habitualmente en criptomonedas, demandada por los ciberdelincuentes.

Figura 8. Ejemplo de correo de sextorsión

3.2. Amenazas al sitio web corporativo

Para las empresas del sector del turismo y ocio el sitio web es un activo muy importante, ya que se trata de su escaparate en Internet, permitiendo ofrecer servicios y productos de manera global, llegando así a un mayor número de clientes. Por lo tanto, un incidente de seguridad relacionado con el sitio web podría perjudicar seriamente a la continuidad de negocio.

Las webs son objetivos de los ciberdelincuentes por diversos motivos, el principal suele ser el beneficio económico, pero también hacerse con información confidencial y utilizar dicha información para perpetrar otros ataques, o simplemente para dañar la imagen de la organización, por lo que disponer de un portal web funcional, seguro y que cumpla las necesidades de los trabajadores y clientes, es imprescindible para las organizaciones.

3

Los incidentes de seguridad, cuyo origen está en el sitio web corporativo, se producen principalmente por los siguientes motivos:

» **Vulnerabilidades no parcheadas [REF - 20]:** entendiendo como vulnerabilidad un fallo o deficiencia en un *software*, que puede ser utilizado por un ciberdelincuente para llevar a cabo acciones maliciosas. Los sitios web pueden contar con vulnerabilidades que si no son parcheadas podrían llegar a ser explotadas, causando un incidente de seguridad.

» **Malas configuraciones:** a través de acciones como permitir contraseñas simples, no aplicar sistemas de verificación tipo *captcha* o mostrar más información que la estrictamente necesaria cuando se produce un error, pudiendo estas malas prácticas suponer el origen de un incidente de ciberseguridad **[REF - 21].**

» **Errores de diseño:** produciéndose cuando una web no está diseñada siguiendo unos estándares de seguridad, como el elaborado por la Fundación OWASP **[REF - 22].** Esto origina que la web contenga errores de diseño, los cuales podrían ser la puerta de entrada a nuestro portal web.

Si finalmente estos errores de seguridad dan lugar a un incidente, podrían tener lugar varias situaciones que comprometan la seguridad y privacidad de la empresa, y por ende, de sus clientes:

» **Fugas de información:** lo que puede dar lugar a la pérdida de confidencialidad de la misma, siendo accesible por personas no autorizadas **[REF - 23].** Estas fugas de información pueden dar lugar a sanciones económicas, debido a un incumplimiento de la LOPDGDD, o a extorsiones por parte de los ciberdelincuentes, entre otros incidentes. En cualquier caso, siempre van a tener un impacto negativo en la imagen y reputación de la organización.

» **Ataques de denegación de servicio [REF - 24] o DoS**, por sus siglas en inglés (*Denial of Service*), que tienen por objetivo dejar un servidor inoperativo. Como consecuencia, este tipo de ataques provocan que tanto clientes como trabajadores no puedan interactuar con el sitio web de forma normal, lo que puede afectar gravemente a la continuidad del negocio.

» ***Defacement* [REF - 25]:** ataque que consiste en cambiar la apariencia de la web corporativa por otra a elección del ciberdelincuente con diversos motivos, como:

- Dañar la imagen de una organización, generando así desconfianza entre sus clientes.
- Alojar un sitio falso, con el fin de ganar dinero, por ejemplo, una página de phishing de una entidad bancaria.
- Distribuir malware o contenido catalogado como spam.
- Llevar a cabo acciones de vandalismo, como enviar mensajes de protesta.

También hay que tener en cuenta que cuando un ciberdelincuente vulnera la seguridad del sitio web corporativo, puede llegar a comprometer otros sistemas de la organización, como el correo electrónico, o dispositivos, como ordenadores o aparatos IoT (*Internet of Things*), etc.

3.3. Amenazas en redes sociales

Hoy en día las redes sociales son una herramienta de gran valor para el sector del turismo y ocio, permitiendo dar a conocer sus productos o servicios de una manera muy visual e interactiva, y a la vez estableciendo un trato más cercano con los actuales o potenciales clientes.

La publicación de imágenes y vídeos de experiencias en tiempo real son un escaparate digital para muchas empresas de este sector, que se valen de estas aplicaciones para llegar a un gran número de usuarios, de una manera mucho más personal, en comparación con cómo se presenta una empresa en una página web.

Pero en este escenario tan ventajoso no podemos ignorar que muchas veces las redes sociales son un blanco fácil para los ciberdelincuentes, sobre todo si como administradores desconocemos los riesgos asociados a su uso. Debemos prestar especial atención a ciertas campañas maliciosas que se llevan a cabo a través de las redes sociales, como:

- los fraudes por suplantación **[REF - 26]** de clientes o proveedores,
- las campañas de *malware* **[REF - 27]**,
- las campañas de *phishing* **[REF - 28]**.

3.4. Amenazas en redes inalámbricas

En los últimos años, muchos negocios del sector del turismo y ocio han decidido incluir entre los servicios que ofrecen a sus clientes la posibilidad de conectarse a un punto de acceso wifi gratuito mientras se encuentran en sus instalaciones. Esta acción, aunque parezca trivial, entraña varios aspectos legales y técnicos que es conveniente revisar cuando se plantea ofrecer este servicio. A los riesgos y amenazas propios de redes cableadas, hay que añadir los inherentes a las redes wifi **[REF - 29]**, como pueden ser los siguientes:

- **Denegación de servicio (DoS):** se trata de incapacitar la infraestructura inalámbrica a través de peticiones de servicio masivas a los puntos de acceso, provocando que los sistemas se vean incapaces de atender todas las peticiones y, por lo tanto, el fallo del servicio.

3

» ***Man-in-the-Middle:*** se basa en que el ciberdelincuente se sitúa entre el emisor y el receptor de la información, suplantando una de las partes y haciendo creer a la otra que está hablando con el legítimo destinatario de la comunicación.

» **Ataques de fuerza bruta:** método que consiste en hacer uso de todas las contraseñas posibles, y cuya finalidad es averiguar las claves de la comunicación o de las que dan acceso a la red wifi.

» ***Eavesdropping*:** consiste en la captura de tráfico de red no autorizado a través de alguna herramienta, como por ejemplo, antenas de gran alcance, realizando así una escucha ilegal o furtiva de la comunicación interceptada, con el objetivo de hacerse con la información que se transmite.

» **MAC *spoofing*:** se trata de suplantar la dirección MAC de un dispositivo con acceso a un determinado punto de acceso.

3.5. Otras amenazas del sector

En el sector del turismo y ocio, con la llegada de la temporada alta, se multiplica el volumen de operaciones de manera considerable. La rapidez en la gestiones y la alta demanda de servicios son el ambiente perfecto para llevar a cabo alguno de los fraudes más comúnmente asociados a este sector.

3.5.1. Transferencias bancarias o cheques sin fondos

En los fraudes asociados a estas formas de pago las reservas siempre se realizan a través de Internet. En el caso de las transferencias bancarias, dado que estas operaciones no son inmediatas, los ciberdelincuentes aprovechan el servicio y después anulan el pago. Cuando se verifican los fondos los ciberdelincuentes ya han abandonado el alojamiento o servicio. En ocasiones, los ciberdelincuentes envían por correo un justificante fraudulento para intentar convencer a la víctima de que han realizado la transferencia, pero en realidad no se ha llevado a cabo tal operación.

En el caso de los cheques sin fondo, estos se envían y, a continuación, los ciberdelincuentes cancelan el viaje y solicitan la devolución del importe que nunca pagaron. Lo habitual es que un supuesto cliente o empresa de viajes extranjera contacte con el establecimiento para hacer una reserva de los servicios. Al poco tiempo, dicho establecimiento recibe un cheque de un banco extranjero con el pago de un importe muy superior al presupuestado.

Al tratarse de una transferencia internacional, las entidades nacionales pueden tardar entre tres y cuatro días en validar el pago mediante el cheque. Cuando el establecimiento lleva el talón a su entidad reciben el ingreso en cuenta del importe, viendo entonces reflejado el pago y procediendo, como de costumbre, a autorizar el servicio.

3

Posteriormente, el supuesto cliente cancela la reserva antes de que se agote el plazo de verificación y solicita la devolución del importe. En este caso, el establecimiento accede a la devolución, pero cuando se completa la verificación y se comprueba que no había fondos, el supuesto cliente ya es ilocalizable.

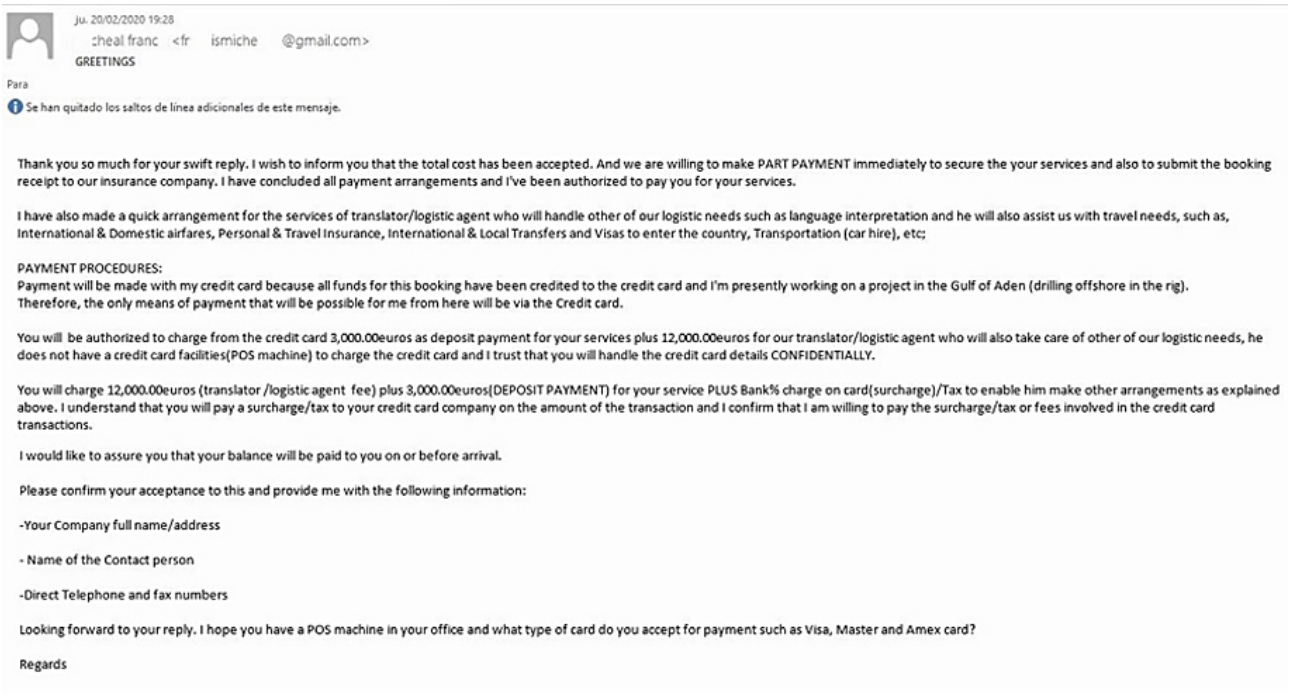
3.5.2. Pagos con tarjetas robadas o ajenas

Cuando se trata de tarjetas robadas el fraude es más difícil y largo de detectar, y permite al defraudador utilizar los servicios durante más tiempo. Este tipo de tarjetas se obtienen en mercados negros, como la *deep web*, y suelen pertenecer a personas de otros países. Cuando el afectado denuncia el robo o los cargos, generalmente ya han transcurrido varios días, y es imposible seguir la pista al ciberdelincuente.

3.5.3. Fraude en las reservas vacacionales

En ciertas ocasiones, los intentos de compra fraudulenta a través de tarjetas robadas o falsas suelen ser detectados por los programas de gestión de reservas que rechazan estas operaciones. Es por esto que los ciberdelincuentes utilizan la ingeniería social para engañar al personal encargado de realizar las reservas.

La siguiente imagen muestra un caso real donde el ciberdelincuente, en la gestión de una reserva para un grupo de viajeros, trata de que el hotel pague a un supuesto guía, el cual ya estaría contratado, pero al que él no podría pagar directamente. En este caso, el estafador se vale de hacer pensar al personal que podría perder esa importante reserva si no accediesen al pago del guía.



ju. 20/02/2020 19:28
:heal franc <fr ismiche @gmail.com>
GREETINGS

Para

Se han quitado los saltos de línea adicionales de este mensaje.

Thank you so much for your swift reply. I wish to inform you that the total cost has been accepted. And we are willing to make PART PAYMENT immediately to secure the your services and also to submit the booking receipt to our insurance company. I have concluded all payment arrangements and I've been authorized to pay you for your services.

I have also made a quick arrangement for the services of translator/logistic agent who will handle other of our logistic needs such as language interpretation and he will also assist us with travel needs, such as, International & Domestic airfares, Personal & Travel Insurance, International & Local Transfers and Visas to enter the country, Transportation (car hire), etc;

PAYMENT PROCEDURES:
Payment will be made with my credit card because all funds for this booking have been credited to the credit card and I'm presently working on a project in the Gulf of Aden (drilling offshore in the rig). Therefore, the only means of payment that will be possible for me from here will be via the Credit card.

You will be authorized to charge from the credit card 3,000.00euros as deposit payment for your services plus 12,000.00euros for our translator/logistic agent who will also take care of other of our logistic needs, he does not have a credit card facilities(POS machine) to charge the credit card and I trust that you will handle the credit card details CONFIDENTIALLY.

You will charge 12,000.00euros (translator /logistic agent fee) plus 3,000.00euros(DEPOSIT PAYMENT) for your service PLUS Bank% charge on card(surcharge)/Tax to enable him make other arrangements as explained above. I understand that you will pay a surcharge/tax to your credit card company on the amount of the transaction and I confirm that I am willing to pay the surcharge/tax or fees involved in the credit card transactions.

I would like to assure you that your balance will be paid to you on or before arrival.

Please confirm your acceptance to this and provide me with the following information:

-Your Company full name/address

- Name of the Contact person

-Direct Telephone and fax numbers

Looking forward to your reply. I hope you have a POS machine in your office and what type of card do you accept for payment such as Visa, Master and Amex card?

Regards

Figura 9. Correo ejemplo de estafa en reserva vacacional

4 MEDIDAS DE CIBERSEGURIDAD PARA EL SECTOR

El sector del turismo y ocio se enfrenta a grandes amenazas en materia de ciberseguridad. Una brecha de seguridad puede ocasionar una pérdida de confianza por parte de los clientes, daño a la reputación de la marca, pérdidas económicas y perjuicios legales. Pese a que estos ataques crecen exponencialmente, muchos de estos riesgos pueden ser evitados o al menos controlados, minimizando así su impacto, si aplicamos ciertas **medidas de ciberseguridad** y, sobre todo, el **sentido común**.

4.1. Medidas para el correo electrónico

Considerando los fraudes a través del correo electrónico más utilizados por los ciberdelincuentes, es importante tener en cuenta las principales medidas de ciberseguridad, que pueden implementarse en las organizaciones, para evitar o minimizar los efectos de este tipo de ataques:

» Hay que asegurarse de que **los correos proceden de un origen confiable**, aunque los ciberdelincuentes pueden utilizar la técnica conocida como *e-mail spoofing* para suplantar direcciones legítimas. Por ello, también se debe revisar con detalle el cuerpo del mensaje, verificando que esté bien redactado y que el texto sea coherente. Aun con estas comprobaciones se puede seguir teniendo dudas sobre la legitimidad de un correo **[REF - 30]**. En estos casos, puede ayudar llevar a cabo el análisis de sus cabeceras.

» En relación con el punto anterior, en los fraudes en los que se solicita realizar algún tipo de pago, el cambio de cuenta para el ingreso de nómina o cualquier solicitud que implique movimientos de dinero, se debe **verificar la acción con la fuente que la solicita**. Esta comprobación se debe hacer **por otro medio distinto al correo electrónico**, bien sea una llamada telefónica, una videollamada o cualquier método en el que se pueda verificar la legitimidad de la acción solicitada.

» En ocasiones, la organización puede verse afectada por algún *ransomware* que haya sigo distribuido por correo electrónico. **En ningún caso se debe pagar el rescate.** Para minimizar el impacto de este tipo de ataques se deben realizar copias de seguridad de forma periódica de los datos del negocio. Estas copias de seguridad deben alojarse en un servidor diferente al que está contenida la información. También resulta conveniente desconectar el equipo infectado lo antes posible de la red para evitar que el ataque pueda propagarse al resto de equipos de la organización.

A continuación, se resaltan los aspectos más relevantes que deben ser considerados a la hora de identificar la legitimidad de un correo electrónico.

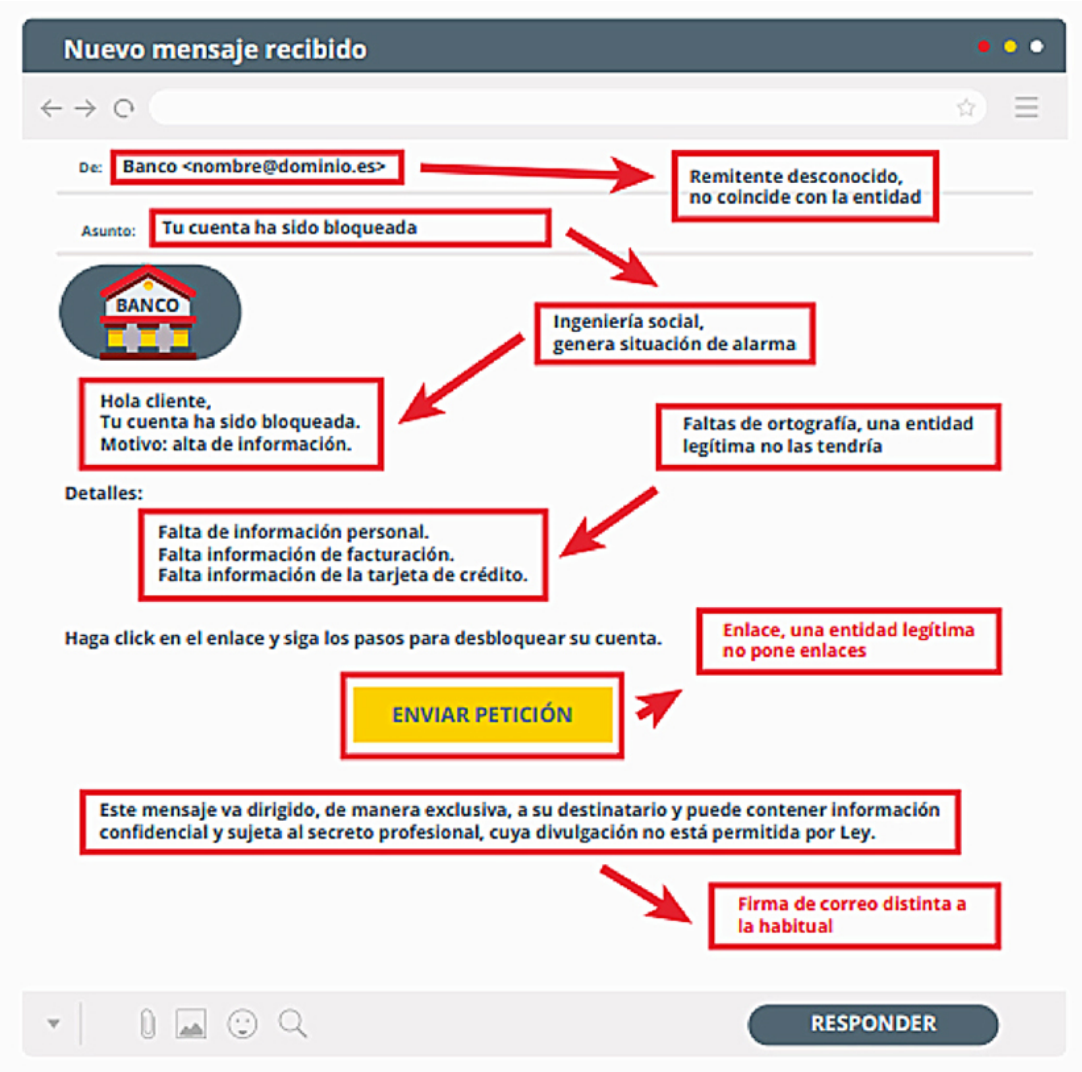


Figura 10. Modelo de correo fraudulento

4.2. Medidas para el sitio web corporativo

En ocasiones, las organizaciones tienen una política de actualización de sus sitios web corporativos deficiente, lo que puede conllevar diferentes vulnerabilidades, que los ciberdelincuentes pueden aprovechar para conseguir sus objetivos. Por ello, la primera medida consiste en mantener el **sitio web actualizado** y que cuente con, al menos, un conjunto mínimo de medidas de protección.

Para proteger el portal web corporativo **[REF - 31]**, y así reducir su nivel de vulnerabilidad y evitar el compromiso de la privacidad y seguridad de la empresa, se debe contar con una política de seguridad **[REF - 32],** que al menos contemple los siguientes puntos:

» **Tener instalado un certificado SSL [REF - 33]**, también conocido como certificado web. Este certificado sirve para proteger las comunicaciones que se establecen entre la web corporativa y el dispositivo del cliente, evitando

que los ciberdelincuentes puedan robar la información en tránsito, como por ejemplo, nombres de usuario y contraseñas. Esta medida siempre es recomendable, ya que muchos navegadores marcan como inseguros los sitios web sin certificado SSL, con un cifrado anticuado, firmados por una entidad no reconocida o que cuenten con un certificado caducado. Además, también sirven para **identificar la web de forma inequívoca**, generando así confianza entre los clientes.

» **Tener al día las actualizaciones de seguridad** del gestor de contenidos o CMS, por sus siglas en inglés *Content Management System*, y sus complementos. La actualización de este *software* debe ser considerada una tarea prioritaria a realizar, tanto si la gestión del sitio web se desarrolla en la empresa como si se realiza por parte de un tercero. Estas aplicaciones publican regularmente actualizaciones de seguridad que corrigen las últimas vulnerabilidades descubiertas. Siempre se debe contar con la última versión disponible tanto del CMS como de los *plugins* y temas utilizados.

» **Utilizar contraseñas robustas** **[REF - 34]**. Las contraseñas de acceso al *backend* del sitio web corporativo deben ser lo más robustas posibles. Para evitar utilizar credenciales de acceso débiles es recomendable establecer mecanismos que no permitan utilizar contraseñas sin unos mínimos de seguridad. Para dotar de un extra de seguridad se puede establecer un mecanismo por el que, ante determinados intentos erróneos de acceso, se inhabilite al usuario asociado durante un determinado tiempo, que se incrementará exponencialmente si continúan los intentos fallidos. Además, se puede habilitar un factor de autenticación adicional **[REF - 35]**, que solamente deberá conocer el usuario legítimo, como puede ser una clave OTP (*One Time Password*).

» **Realizar copias de seguridad** **[REF - 36]**. Las copias de seguridad son indispensables en cualquier entorno corporativo y el sitio web de la empresa no es una excepción. Se deben realizar copias de seguridad periódicas y almacenarlas en un entorno seguro, además de comprobar que pueden restaurarse.

» **Utilizar sistemas de respaldo.** Los sistemas de respaldo permiten que la web corporativa siga operativa en caso de incidente de seguridad o fallo del sistema. El sistema de respaldo debe estar ubicado en un servidor independiente, que pueda ser activado cuando el servidor principal no pueda ofrecer el servicio.

» **Utilizar sistemas *captcha*** **[REF - 37]**. Estos sistemas impiden que los bots o programas automatizados puedan interactuar con determinadas partes de la web corporativa, como pueden ser el área de comentarios o la página de inicio de sesión.

» **Realizar una gestión de registros** **[REF - 38]** (*logging*). Un sistema de gestión de registros o logs guarda los eventos más importantes que tienen lugar en el sitio web corporativo. Así, en caso de incidente de seguridad, se podrá investigar lo sucedido para mitigar el incidente y tomar las medidas oportunas para evitar que suceda de nuevo.

» **Tener instalados entornos de producción y prueba.** Cuando se aplica una actualización de seguridad o cualquier otro cambio significativo

en el sitio web corporativo es recomendable realizarlo previamente en un entorno controlado, de modo que, ante cualquier fallo imprevisto, el entorno de producción no se vea afectado. Por ello, es importante disponer de dos entornos bien diferenciados: uno de pruebas o preproducción y el sitio web funcional y público o producción.

» **Asegurar pagos online seguros.** Si el portal web permite a los clientes comprar de forma online, se deben **implementar métodos seguros** **[REF - 39]**, como los TPV virtuales, cuyas comunicaciones viajen cifradas, o contratar una entidad intermediadora reconocida, como PayPal o Google Pay.

» **Asegurar el cumplimiento legal y normativo.** No cumplir con la ley vigente puede derivar en distintas sanciones por incumplimiento normativo, además de generar desconfianza entre los clientes. Para cumplir con la normativa se deben tratar los datos personales de acuerdo a la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) **[REF - 40],** la Ley de Servicios de la Sociedad de la Información (LSSI) y la Ley de Propiedad Intelectual o (LPI). Además, se debe cumplir cualquier otro tipo de normativa vigente **[REF - 41]** que afecte a la actividad de la empresa.

4.3. Medidas para las redes sociales

Debido al uso cada vez mayor de las redes sociales por parte del sector del turismo y ocio, es importante asegurarse de no ser víctimas de un incidente de seguridad relacionado con la utilización de las mismas. Para ello, se pueden adoptar una serie de medidas de carácter preventivo:

» **Utilizar contraseñas de acceso robustas.** El binomio usuario y contraseña permite acceder a la administración de las redes sociales, de ahí la importancia de utilizar una contraseña fuerte que no sea fácilmente descifrable, y habilitar siempre que sea posible el doble factor de autenticación. Un acceso no autorizado por parte de un ciberdelincuente podría permitirle conseguir la información del perfil, comunicarse con clientes o publicar en nombre de la empresa, lo que podría ocasionar fugas de información y graves consecuencias en la reputación, entre otros incidentes.

» **Realizar una correcta configuración de la privacidad**. Todas las redes sociales cuentan con parámetros de privacidad que disponen de distintos niveles de restricción. Esto permite encontrar un punto intermedio entre funcionalidad y seguridad para utilizar las redes sociales de manera efectiva e interactuar con los clientes, sin descuidar la seguridad y privacidad del perfil.

» **Elegir un responsable de publicación**. Si bien es una buena opción que los empleados aporten ideas para llevar a cabo acciones que aumenten la popularidad de la empresa, no es una buena práctica permitir el acceso y publicación de forma indiscriminada. Con esta práctica, a la larga, la imagen de la empresa puede verse dañada, además de aumentar el riesgo de sufrir un incidente de seguridad.

» **Llevar a cabo restricciones de acceso**. Existen aplicaciones que por diferentes motivos (gestión, estadísticos, publicitarios, etc.) solicitan acceso a los diferentes perfiles de las redes sociales. Ante esta situación es recomendable analizar detenidamente dichos accesos antes de habilitarlos. De lo contrario, esta práctica puede suponer un riesgo para la privacidad, al permitir el acceso a determinados datos que pueden ser privados (como información de seguidores o clientes) o la publicación de contenido no supervisado por la empresa.

» **Estar al día de las ciberamenazas**. La suscripción al boletín de avisos de Protege tu empresa **[REF - 42]**, de INCIBE, permite estar al día de las amenazas que pueden afectar a las empresas, facilitando la prevención y protección ante incidentes de seguridad.

» **Fomentar la formación y concienciación de los empleados**. La falta de formación **[REF - 43]** en materia de ciberseguridad puede conllevar una mala gestión de las redes sociales por parte de su administrador. Un error frecuente y, por tanto, una práctica de riesgo, es la publicación de información privada, ya que los ciberdelincuentes utilizan estas aplicaciones como fuente de información para planificar y llevar a cabo sus ataques.

» **Tener precaución a la hora de seguir enlaces y descargar adjuntos** **[REF - 44]**. Es muy habitual la difusión de *malware* a través de redes sociales mediante documentos adjuntos, mensajes dentro de la propia red o sitios web de terceros. En caso de que un enlace dirija a cualquier web que solicite cualquier tipo de dato personal o bancario, es recomendable verificar que dicha web es legítima y comprobar su certificado de seguridad, asegurándose de que corresponde con el sitio al que se está accediendo.

Además, hay que tener en cuenta una serie de **acciones a evitar** a la hora de publicar en redes sociales:

» Dar información confidencial o sujeta a propiedad intelectual.

» Lanzar comentarios inoportunos, negativos o inapropiados, como por ejemplo, quejas laborales.

» Emitir juicios de valor.

» Enfrascarse en discusiones sin sentido, insultar, amenazar o acosar.

» Propagar noticias falsas.

4.4. Medidas para redes inalámbricas

Uno de los servicios más demandados por los clientes, a la hora de utilizar los servicios relacionados con el sector del turismo y ocio, suele ser disponer de una red wifi gratuita **[REF - 45]**, bien sea en el hotel donde se alojan, en la cafetería donde realizan una consumición o en cualquier otro lugar. Por este motivo, es importante que las empresas que ofrezcan este servicio adicional tengan en consideración las siguientes medidas de seguridad:

» **Mantener actualizado el *firmware* del *router*** o del punto de acceso a la última versión disponible.

» **Cambiar las credenciales de acceso por defecto del panel de administración del *router*** o punto de acceso, utilizando contraseñas seguras y robustas.

» Usar, como mínimo, un **cifrado WPA2-PSK** para la transmisión de datos entre el *router* y el dispositivo del cliente. Con ello, se evita que otros usuarios de la red vean lo que transmite el cliente.

» Cambiar el nombre que viene por defecto de la red.

» Establecer **mecanismos de control parental** para evitar el acceso a sitios web perjudiciales para los menores.

» Asegurar que debe ser **independiente la red wifi** ofrecida a los clientes del resto de redes de las que disponga el negocio, como la red local.

» La contraseña a la red wifi de los clientes debe ser totalmente diferente a la utilizada para el resto de redes de la empresa.

» Aunque la contraseña **[REF - 46]** se ofrezca de manera gratuita a los clientes, esta debe ser cambiada de forma periódica.

» Fuera de horario es recomendable **apagar la red wifi de clientes** para evitar que se utilice mientras el establecimiento permanece cerrado.

» Siempre que sea posible, se deberá **ocultar el SSID del resto de redes wifi de la empresa**.

4.5. Otras medidas específicas del sector

Además de todas las medidas mencionadas, dentro de este sector también aplican un conjunto de recomendaciones básicas que, de forma preventiva, pueden evitar que se produzcan incidentes de ciberseguridad que impacten en el negocio. Estas recomendaciones son relativas a la utilización de los métodos habituales de pago, las oficinas de trabajo y los destinos turísticos inteligentes seguros.

4.5.1. Medidas para métodos de pago

El sector del turismo y ocio, debido a la alta demanda de sus servicios, lleva a cabo un gran número de gestiones relacionadas con los métodos de pago, propiciando un ambiente óptimo para los ciberdelincuentes. Por este motivo, es importante tener en cuenta una serie de medidas de ciberseguridad que eviten o minimicen los riesgos asociados a estos procesos.

4.5.1.1. Identificación segura de usuarios

Se trata de un punto **clave para que el usuario y la empresa establezcan una relación comercial de confianza desde el inicio** y es la primera barrera defensiva contra el fraude.

Para llevarla a cabo se puede contar con plataformas o portales de identificación seguros, donde el usuario tenga que autentificarse mediante contraseña, pero añadiendo una capa extra de seguridad, como por ejemplo, la autenticación multifactor **[REF - 47]**.

De esta forma, la empresa confirma la identidad de los usuarios, que han tenido que superar unos mecanismos de validación, aportando información que solo ellos conocen o poseen, como su huella dactilar, una clave generada a través de su teléfono móvil, etc.

4.5.1.2. Establecimiento de políticas de formas de pago y cobro

Una buena práctica consiste en adoptar unas **políticas estrictas en el apartado de cobros a clientes y pagos a proveedores,** a través de plataformas electrónicas con reputación demostrada y seguridad actualizada. Estas deben adaptarse al modelo de negocio, ofreciendo al cliente diversas formas de pago electrónico, verificadas y seguras.

Si el cliente no dispone de las formas de pago ofrecidas, y busca efectuar el pago de otra manera o modificar un pago realizado, debemos contar al menos con una persona con experiencia y conocimientos suficientes en ese campo, para que analice esta situación y dé una respuesta al cliente, de forma que nunca se pierdan las medidas de seguridad establecidas en la política, adoptando los mecanismos de comunicación oportunos para verificar la identidad de la persona, siempre usando los medios oficiales para que todo quede reflejado convenientemente y dando los plazos adecuados para poder realizar las comprobaciones necesarias.

A *priori*, si se ha desarrollado una política estricta de formas de pago y cobros, no se deben realizar cobros, pagos, devoluciones o modificaciones fuera de los canales establecidos o por procedimientos no habituales, aunque de entrada suponga tener quejas por parte de los clientes.

En muchas ocasiones, las empresas automatizan algunos procesos, con el fin de agilizar los procedimientos de cara a una mayor satisfacción por parte del cliente, como las devoluciones económicas, que a veces, debido a esta celeridad, se realizan sin hacer las oportunas comprobaciones por parte de la entidad bancaria.

Si se marcan unos plazos de devolución y unos mecanismos para implementarlos a través de las plataformas de pago, y se informa a los clientes de estas políticas, estos no tendrán problema en esperar mientras se les mantenga informados del estado de su solicitud. Si por el contrario el cliente requiere rapidez en la devolución y lo solicita a través de medios no contemplados previamente, se le debe informar de las políticas establecidas y no salir de ellas.

4.5.1.3. Pasarelas de pago seguras

Las pasarelas de pago son las plataformas que se utilizan en los negocios para facilitar el pago de sus clientes. La pasarela debe ser confiable, intuitiva y suficientemente clara en la información que transmite.

Actualmente, la mayoría de plataformas que existen podrían considerarse seguras. Sin embargo, algunas presentan más características de seguridad que otras, como es el caso del sistema de verificación de direcciones, que solicita al comprador la dirección fiscal a la que está vinculada la tarjeta, lo que permite identificar al comprador como titular de la misma, creando, por tanto, una barrera adicional contra el fraude.

Todas las plataformas de pago deben adaptarse a la legislación vigente y superar determinadas pruebas, entre las que destacan:

- Realizar tests de seguridad regularmente.
- Cifrar la transmisión de los datos de las tarjetas.
- Mantener una configuración que proteja los datos y cambiar los parámetros de seguridad que vienen por defecto.

También hay que tener en cuenta que la plataforma de pago disponga de un servicio de soporte, con el que se pueda contactar rápidamente en caso necesario, y que mantenga su plataforma actualizada.

4.5.2. Medidas para una oficina segura

Como medidas de ciberseguridad adicionales, hay que tener en cuenta una serie de cuestiones que van a permitir a las empresas relacionadas con el sector del turismo y ocio disponer de oficinas con unos niveles de seguridad confiables.

4.5.2.1. Redes wifi

Es importante que las oficinas dispongan de un *firewall* **[REF - 48]**, cuya función es prevenir y proteger la red privada de la organización de intrusiones o ataques externos, bloqueando su acceso. Un *firewall* puede ser implementado tanto por *software* como por *hardware*. Entre sus principales ventajas destacan:

- Es capaz de **permitir o bloquear el tráfico entre redes y equipos de una misma red**, en función de unas reglas previamente establecidas. De esta forma, se evita que usuarios no autorizados accedan a redes privadas.
- Supervisa la comunicación entre los equipos e Internet.
- Visualiza y bloquea aplicaciones que puedan suponer un riesgo.
- **Advierte de intentos de conexión** desde otros equipos.

4.5.2.2. Empleados seguros

A la hora de contratar a los empleados de una empresa se debe tener en cuenta una serie de recomendaciones, porque en caso de no valorar ciertos aspectos, el negocio podría ser víctima de un ataque desde dentro.

Estos ataques internos se pueden llevar a cabo a través de los denominados ***insiders***, que se trata de empleados que comprometen la organización para la que trabajan, por motivaciones económicas y/o personales. Esta figura es de especial relevancia, debido a que su conocimiento sobre la empresa (información, procesos y tecnología utilizada), puede asegurar el éxito del ataque:

- Es importante que durante la contratación de cualquier empleado se firmen **acuerdos de confidencialidad y protección de datos**.

- Todos los empleados deben conocer las políticas de la empresa en materia de ciberseguridad, siendo recomendable realizar cursos de formación en caso necesario.

4.5.2.3. Puesto de trabajo seguro

Cualquier puesto de trabajo es susceptible de tener un incidente de ciberseguridad, pero evitarlo o minimizar su impacto es posible si se tienen en cuenta una serie de recomendaciones:

- Todos **los puestos de trabajo deben contar únicamente con los permisos estrictamente necesarios** que requiera la labor que va a desempeñar un empleado allí. Una mala gestión de los permisos podría permitir a un empleado instalar un programa no autorizado por la empresa y, a raíz de la instalación de ese programa, sufrir un incidente de seguridad, bien por una vulnerabilidad no parcheada en el programa que se instala o simplemente por el hecho de compartir información de la empresa sin conocimiento del empleado.

- Es importante que **no se compartan puestos de trabajo**, y en caso de tener que compartirse, es recomendable que cada empleado tenga **cuentas diferentes**.

- Se debe limitar a lo estrictamente necesario el uso de servicios de almacenamiento online.

- Se debe **restringir la conexión de dispositivos no autorizados a los equipos**, como pueden ser *pendrives*, ya que estos dispositivos pueden servir como vector de entrada en un incidente de seguridad, al estar infectados por *malware*, o provocar una fuga de información, en caso de que un empleado copie en ellos información sensible de la empresa y luego los pierda.

- Se debe tener un **control sobre las páginas que visitan** los empleados, tratando de bloquear todas aquellas páginas maliciosas.

Por otra parte, los empleados también deben seguir una serie de recomendaciones y buenas prácticas:

» **Mantener la confidencialidad**.

» **Notificar cualquier incidente de seguridad,** como pueden ser alertas generadas por el antivirus, llamadas recibidas que sean sospechosas, pérdida o robo de algún dispositivo corporativo, borrado accidental de ficheros, comportamientos anómalos, etc.

» No compartir ni publicar contraseñas.

» Bloquear el puesto de trabajo al ausentarse de este.

» No alterar la configuración del equipo.

4.5.2.4. Proveedores de servicios TIC

Normalmente, las empresas contratan ciertos servicios a terceros **[REF - 49]**, como pueden ser el diseño y mantenimiento de la web, almacenamiento en la nube o cualquier otro servicio, pero el hecho de tener estos servicios contratados no exime de exigir al proveedor de los mismos el cumplimiento de medidas ciberseguridad, teniendo en cuenta que es importante:

» que los proveedores de servicios tomen las debidas medidas de ciberseguridad para alinearse y respaldar la política de ciberseguridad de la empresa,

» conocer cómo van a actuar los proveedores de los servicios, en caso de ser víctimas de un incidente de seguridad relacionado con sus servicios.

4.5.3. Destinos turísticos inteligentes y seguros

Las nuevas tecnologías, como el IoT (*Internet of Things*), el *big data* o la inteligencia artificial, han llegado para quedarse **[REF - 50]**. Su utilización dota a las empresas de ventajas competitivas, una mayor productividad y una mejor rentabilidad de sus procesos, razones más que suficientes para continuar su tendencia en alza.

No obstante, las nuevas tecnologías también implican riesgos. Un buen ejemplo son los **dispositivos IoT**, utilizados por ejemplo en la domotización de alojamientos y otros establecimientos turísticos, que debido a su auge y su gran capacidad de interconexión, se convierten en un objetivo perfecto para los ciberdelincuentes. Algunas de las **principales amenazas** a las que pueden estar expuestos son:

» **Ataques de fuerza bruta** para obtener claves de acceso al dispositivo.

» **Ataques de denegación de servicio** que produzcan indisponibilidad de los dispositivos por saturación.

» **Utilización como punto de entrada hacia otros dispositivos del entorno**, ya que por defecto suelen estar menos fortificados y son más accesibles desde el exterior de la red donde se encuentran.

» **Obtención de datos** de carácter personal de los usuarios, como hábitos de uso, contraseñas de acceso a servicios web e incluso datos de tarjetas de crédito.

Para reducir el riesgo de estas amenazas se pueden implementar una serie de **medidas**:

» **Tener una política de actualizaciones de los dispositivos**, importante para minimizar el riesgo de que estos sean vulnerables.

» **Implementar autenticación, control de accesos y administración**, evitando las contraseñas predeterminadas. Una contraseña robusta para acceder a la configuración del dispositivo es una buena medida contra accesos no deseados, así como administrarlos (en caso de ser posible) solo de forma local.

» **Asegurar la protección de los datos almacenados**, controlando qué datos almacenados dentro de los dispositivos se envían a los fabricantes.

» **Usar protocolos seguros** en todas las comunicaciones con otros dispositivos y equipos.

» **Bloquear puertos**, siempre y cuando sea posible, desactivando todos aquellos que no se vayan a utilizar para evitar brechas de seguridad.

» **Establecer un plan de continuidad del servicio**, teniendo un dispositivo que pueda trabajar de forma autónoma, es decir, sin supervisión remota por si se produce un fallo en la red. También es importante que el dispositivo cuente con un sistema de logs que almacene datos, en caso de producirse un fallo, para investigar las causas del mismo.

Por su parte, el ***big data*** **[REF - 51]** y la **inteligencia artificial** pueden ser grandes aliados para que cualquier organización ofrezca productos más personalizados a sus clientes, gracias a la recopilación de grandes volúmenes de datos y su análisis, en función de las necesidades del negocio.

En este caso, al basarse en el análisis de miles de datos, entre los que se pueden encontrar **datos de carácter personal**, su correcto y adecuado tratamiento es una medida imprescindible para garantizar que se cumplen los principios básicos de **confidencialidad, integridad y disponibilidad de la información tratada**, contribuyendo además a la seguridad del negocio, así como evitar consecuencias legales por incumplimiento de la LOPDGDD y/o daños en la reputación del negocio.

Además, hay que tener en cuenta que los sistemas basados en inteligencia artificial deben mantenerse actualizados y debidamente protegidos para evitar que sean vulnerables a determinados ataques.

De forma general, una buena **política de seguridad**, implementada en función de las tecnologías utilizadas en el negocio, junto con la adecuada **formación y concienciación** de todos los empleados, pueden hacer que las empresas se beneficien de las ventajas que estas tecnologías disruptivas están ofreciendo, evitando ser víctimas de un incidente de ciberseguridad.

4.6. Reporte y resolución de incidentes

INCIBE pone a disposición de las empresas toda la información necesaria para poder identificar y reportar los incidentes de ciberseguridad que les puedan afectar **[REF - 52]**.

La información facilitada será analizada y gestionada por **INCIBE-CERT** **[REF - 53]**, el centro de respuesta a incidentes de INCIBE, en el que participan activamente agentes de la Oficina de Coordinación Cibernética del Ministerio del Interior, lo que permite trasladar de una forma muy ágil los casos constitutivos de delito telemático a las unidades técnicas de las Fuerzas y Cuerpos de Seguridad del Estado.

5 REFERENCIAS

[REF - 1] **España Digital 2025 -** https://portal.mineco.gob.es/ca-es/ministerio/estrategias/Pagines/00_Espana_Digital_2025.aspx

[REF - 2] **Glosario de términos de ciberseguridad: una guía de aproximación para el empresario -** https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario

[REF - 3] **Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario -** https://www.incibe.es/protege-tu-empresa/guias/ganar-competitividad-cumpliendo-el-rgpd-guia-aproximacion-el-empresario

[REF - 4] **Informe ONTSI -** https://www.ontsi.es/sites/ontsi/files/2020-07/TecnologíasHabilitadorasDigitalesEspañaImpactoSectoresAgroalimentarioTurísticoMedioambiente.pdf

[REF - 5] **Catálogo de empresas y soluciones de ciberseguridad -** https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad

[REF - 6] **Herramienta de autodiagnóstico -** https://adl.incibe.es/

[REF - 7] **Avisos INCIBE -** https://www.incibe.es/protege-tu-empresa/avisos-seguridad

[REF - 8] **Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse -** https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

[REF - 9] **Historias reales: un falso proveedor a mi empresa se la jugó -** https://www.incibe.es/protege-tu-empresa/blog/historias-reales-falso-proveedor-mi-empresa-se-jugo

[REF - 10] **Historias reales: envié correos spam sin saberlo y me han bloqueado -** https://www.incibe.es/protege-tu-empresa/blog/historias-reales-envie-correos-spam-saberlo-y-me-han-bloqueado

[REF - 11] **Descubre los diferentes tipos de malware que pueden afectar a tu pyme -** https://www.incibe.es/protege-tu-empresa/blog/descubre-tipos-malware

[REF - 12] **Busca otro al que engañar, yo no voy a picar -** https://www.incibe.es/protege-tu-empresa/blog/busca-otro-al-enganar-yo-no-voy-picar

[REF - 13] **Historias reales: El timo del falso soporte técnico -** https://www.incibe.es/protege-tu-empresa/blog/historias-reales-el-timo-del-falso-soporte-tecnico

[REF - 14] **¿Microsoft te ha llamado sin haberlo solicitado? -** https://www.osi.es/es/actualidad/blog/2019/04/04/microsoft-te-ha-llamado-sin-haberlo-solicitado

5

[REF - 15] **Historias reales: el fraude del CEO -** https://www.incibe.es/protege-tu-empresa/blog/historias-reales-el-fraude-del-ceo

[REF - 16] **Historias reales: el fraude del CEO tiene un arma nueva, Google Drive -** https://www.incibe.es/protege-tu-empresa/blog/historias-reales-el-fraude-del-ceo-tiene-arma-nueva-google-drive

[REF - 17] **Avisos de seguridad – Fraude de RRHH -** https://www.incibe.es/protege-tu-empresa/avisos-seguridad/fraude-rrhh

[REF - 18] **Ayuda ransomware -** https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware

[REF - 19] **Campaña de correos electrónicos fraudulentos que trata de sextorsionar a sus víctimas -** https://www.incibe.es/protege-tu-empresa/avisos-seguridad/campana-correos-electronicos-fraudulentos-trata-sextorsionar-sus

[REF - 20] **Avisos de seguridad -** https://www.incibe.es/protege-tu-empresa/avisos-seguridad/filtro/vulnerabilidad

[REF - 21] **Medidas de seguridad avanzadas en WordPress II -** https://www.incibe.es/protege-tu-empresa/blog/medidas-seguridad-avanzadas-wordpress-ii

[REF - 22] **Open Web Application Security Project® (OWASP) -** https://owasp.org/

[REF - 23] **¡Fuga detectada, información robada! -** https://www.incibe.es/protege-tu-empresa/blog/fuga-detectada-informacion-robada

[REF - 24] **Medidas de prevención contra ataques de denegación de servicio -** https://www.incibe.es/protege-tu-empresa/blog/medidas-prevencion-ataques-denegacion-servicio

[REF - 25] **Protégete frente al defacement y que no le cambien la cara a tu web -** https://www.incibe.es/protege-tu-empresa/blog/protegete-frente-al-defacement-y-no-le-cambien-cara-tu-web

[REF - 26] **Fraudes online: aprende a identificarlos -** https://www.incibe.es/protege-tu-empresa/blog/fraudes-online-aprende-identificarlos

[REF - 27] **#AprendeCiberseguridad – malware -** https://www.incibe.es/aprendeciberseguridad/malware

[REF - 28] **#AprendeCiberseguridad – phishing -** https://www.incibe.es/aprendeciberseguridad/phishing

[REF - 29] **Protege tu empresa – Guías -** https://www.incibe.es/protege-tu-empresa/guias/seguridad-redes-wifi-guia-aproximacion-el-empresario

[REF - 30] **¿Dudas sobre la legitimidad de un correo? Aprende a identificarlos -** https://www.incibe.es/protege-tu-empresa/blog/dudas-legitimidad-correo-aprende-identificarlos

5

[REF - 31] **Protege tu web -** https://www.incibe.es/protege-tu-empresa/que-te-interesa/protege-tu-web

[REF - 32] **Protección de la página web: políticas de seguridad para la pyme -** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/proteccion-pagina-web.pdf

[REF - 33] **Si tu web cuenta con certificado de seguridad, comprueba que utilizas una versión segura del protocolo TLS -** https://www.incibe.es/protege-tu-empresa/blog/si-tu-web-cuenta-certificado-seguridad-comprueba-utilizas-version-segura-del

[REF - 34] **Día Mundial de las Contraseñas, ¿aún utilizas 123456? -** https://www.incibe.es/protege-tu-empresa/blog/dia-mundial-las-contrasenas-aun-utilizas-123456

[REF - 35] **Dos mejor que uno: doble factor para acceder a servicios críticos -** https://www.incibe.es/protege-tu-empresa/blog/dos-mejor-uno-doble-factor-acceder-servicios-criticos

[REF - 36] **Copias de seguridad: una guía de aproximación para el empresario -** https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

[REF - 37] **¿Humano o bot? Protege tu web con sistemas captcha -** https://www.incibe.es/protege-tu-empresa/blog/humano-o-bot-protege-tu-web-sistemas-captcha

[REF - 38] **Gestión de logs: políticas de seguridad para la pyme -** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/gestion-logs.pdf

[REF - 39] **¿Conoces las pasarelas de pago? ¿Sabes cuál es la más adecuada para tu tienda online? -** https://www.incibe.es/protege-tu-empresa/blog/conoces-las-pasarelas-pago-sabes-cual-mas-adecuada-tu-tienda-online

[REF - 40] **Cómo incluir información legal en tu página web y cumplir con la LOPDGDD -** https://www.incibe.es/protege-tu-empresa/blog/incluir-informacion-legal-tu-pagina-web-y-cumplir-lopdgdd

[REF - 41] **Cumplir la ley, ya seas pyme o autónomo, nunca fue tan fácil -** https://www.incibe.es/protege-tu-empresa/blog/cumplir-ley-seas-pyme-o- autonomo-nunca-fue-tan-facil

[REF - 42] **Suscripción a boletines de INCIBE -** https://www.incibe.es/suscripciones

[REF - 43] **Formación -** https://www.incibe.es/protege-tu-empresa/formacion

[REF - 44] **Fraude y Gestión de la Identidad Online -** https://www.incibe.es/protege-tu-empresa/que-te-interesa/fraude-gestion-identidad-online

[REF - 45] **Seguridad en redes wifi: una guía de aproximación para el empresario -** https://www.incibe.es/protege-tu-empresa/guias/seguridad-redes-wifi-guia-aproximacion-el-empresario

[REF - 46] **¿Cuánto hace que no cambias tus contraseñas? -** https://www.incibe.es/protege-tu-empresa/blog/cuanto-hace-no-cambias-tus-contrasenas

[REF - 47] **Asegura tus cuentas de usuario con la autenticación de doble factor -** https://www.incibe.es/protege-tu-empresa/blog/asegra-tus-cuentas-usuario-autenticacion-doble-factor

[REF - 48] **Firewall tradicional, UTM o NGFW. Diferencias, similitudes y cuál elegir según tus necesidades -** https://www.incibe.es/protege-tu-empresa/blog/firewall-tradicional-utm-o-ngfw-diferencias-similitudes-y-cual-elegir-segun

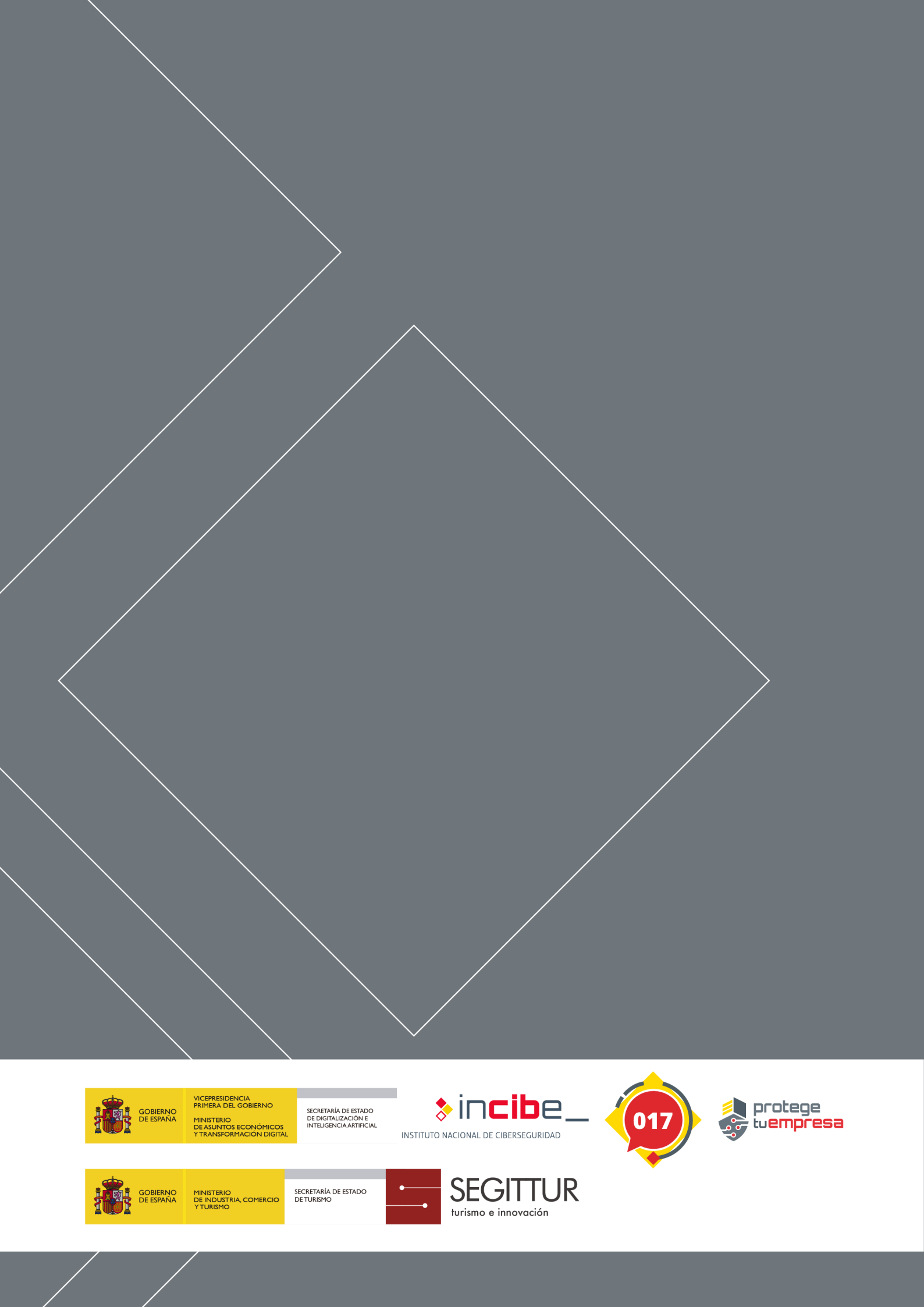
[REF - 49] **Acuerdo pactado, contrato firmado. ¡Protege tu empresa! -** https://www.incibe.es/protege-tu-empresa/blog/acuerdo-pactado-contrato-firmado-protege-tu-empresa

[REF - 50] **Tecnologías disruptivas para la empresa segura -** https://www.incibe.es/protege-tu-empresa/blog/tecnologias-disruptivas-empresa-segura

[REF - 51] **Big Data, IA y analítica predictiva: del dato a la inteligencia de ciberseguridad -** https://www.incibe-cert.es/blog/big-data-ia-y-analitica-predictiva-del-dato-inteligencia-ciberseguridad

[REF - 52] **Reporta tu incidente -** https://www.incibe.es/protege-tu-empresa/reporte-fraude

[REF - 53] **INCIBE-CERT -** https://www.incibe-cert.es


GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa
GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO
SECRETARÍA DE ESTADO DE TURISMO
SEGITTUR
turismo e innovación