MAPA DE CIBERRIESGOS

Grupo de Trabajo de Ciberriesgos de
AGERS e ISMS Forum

agers | Asociación Española de Gerencia de Riesgos y Seguros

isms forum spain

MAPA DE CIBERRIESGOS

Grupo de trabajo de ciberriesgos
de AGERS e ISMS Forum

AGERS - Asociación Española De Gerencia de Riesgos y Seguros

C/Príncipe de Vergara 86, 28006 Madrid

ISBN: 978-84-09-15699-3

COPY-RIGHT: DEP637069924879482906

DEPÓSITO LEGAL: M-35208-2019

COLABORADORES AGERS

Juan Gayá – El Corte Inglés

Alfredo Zorzo – One eSecurity

Belén Medina – Globalvia

Eva Pérez – TRANSFESA

Iván Alcauza

Álvaro González la Calle – AENA

Juan Pedro Gago – Deutsche Bank

COLABORADORES ISMS FORUM

Daniel Largacha, Mapfre.

Francisco Lázaro, Renfe.

Concepción Cordón, EMASA.

Eduardo Lopez, Cyber Strategy, Transformation and Assessments, Deloitte.

Carlos Borrego, Cyber Strategy, Transformation and Assessments, Deloitte.

ÍNDICE

1. INTRODUCCIÓN

La tecnología es algo imprescindible en los negocios y en nuestras vidas. Cada vez está más extendida, es más fácil de utilizar y está al alcance de todos. Nos hace la vida más cómoda y la gestión de las empresas más eficiente. Pero esta tecnología genera nuevos e importantes riesgos.

Este trabajo supone una continuación de la GUÍA DE TERMINOLOGÍA DE CIBERSEGURIDAD, publicada en 2017 y la GUÍA TOP TEN CYBER RISK publicada en 2018, ambas elaboradas en colaboración entre AGERS e ISMS. Además, se sigue manteniendo el objetivo de facilitar la comprensión del riesgo de la tecnología de la información entre todos los perfiles afectados por este tipo de riesgo.

En la primera guía pretendíamos hacer comprensibles, para las personas no expertas en las tecnologías de la información, términos utilizados habitualmente. En la segunda, explicábamos en detalle 10 de los principales riesgos tecnológicos, incidiendo en la causa del incidente y las distintas medidas disponibles para evitarlos o minimizarlos.

En esta ocasión, damos un paso adelante en cuanto a la complejidad del análisis, ya que vamos a valorar este tipo de riesgos en función de su frecuencia e intensidad. Para esto utilizaremos una herramienta habitual en el análisis de los riesgos: el mapa de riesgos.

Este consiste en una matriz que permite mostrar los riesgos según su frecuencia e intensidad. La combinación de estos parámetros permite mostrar una clasificación de la importancia de cada riesgo.

No existe un mapa de riesgos único para todas las empresas. Cada empresa, en función de múltiples características, puede valorar las consecuencias de un incidente de forma diferente. Además, un mapa de riesgos es algo dinámico, cambia con el tiempo dentro de una empresa.

Por este motivo hemos desarrollado dos casos, buscando situaciones relativamente extremas, y buscando que cada uno de los lectores de este documento pueda verse más identificado con uno u otro caso. Por un lado, una empresa con una alta dependencia tecnológica: sin sistemas de información operativos, la actividad se paraliza (venta online de productos informáticos) y por otro, una empresa más tradicional (un pequeño hotel familiar), cuya actividad principal no se sustenta en los sistemas de información.

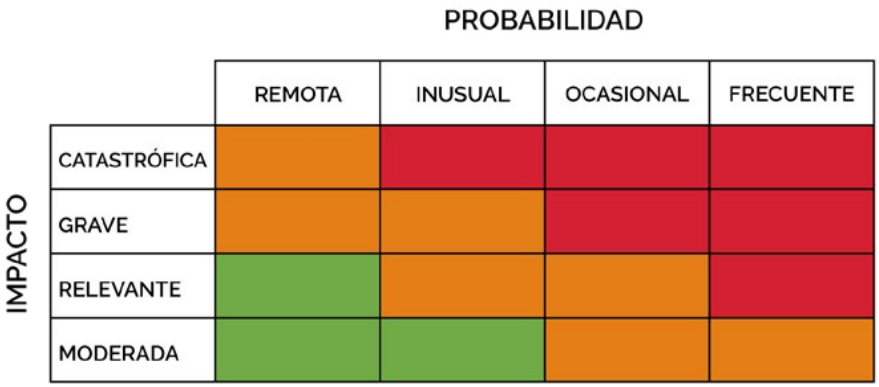
de productos informáticos) y por otro, una empresa más tradicional (un pequeño hotel familiar), cuya actividad principal no se sustenta en los sistemas de información.

El fin último del mapa de riesgos es mejorar la gestión del riesgo de una organización. Los riesgos con una alta probabilidad y una alta importancia deben ser especialmente gestionados para reducir al menos uno de estos parámetros. Por este motivo el documento no termina con la presentación del mapa de riesgos de cada una de las empresas estudiadas, sino que finaliza con un plan para gestionar los riesgos detectados como más peligrosos.

2. QUÉ ES UN MAPA DE RIESGOS

Un mapa de riesgos es una herramienta de **toma de decisiones** que proporciona, de manera visual, una perspectiva de los riesgos de una organización y su orden de prioridad. Su objetivo es mejorar la comprensión del perfil de riesgo de la compañía, la naturaleza y el impacto de sus exposiciones al riesgo.

Para ello, los riesgos identificados que afecten a los **procesos de la empresa**, se representan en una "matriz de riesgos" (o mapa de calor), definida por la probabilidad del suceso y su impacto en la organización.



Ejemplo de mapa de riesgos

Los mapas de riesgos deben de ser consecuentes con el **apetito al riesgo de la organización**, que se define como "la cantidad y el tipo de riesgo que una organización está dispuesta a asumir", según ISO 31000:2009.

Previamente a la elaboración de un mapa de riesgos, deberemos identificar todos los procesos de la organización y elaborar un registro de riesgos objeto de seguimiento, así como los **controles que se aplicarán a los riesgos identificados**.

El registro de riesgos incluirá los niveles de probabilidad e impacto para cada uno de ellos, lo cual se trasladará a una matriz que representará el nivel de riesgo residual después de aplicar los controles establecidos.

En los casos que analizaremos posteriormente, consideramos que se han realizado los controles más comunes para las actividades descritas, previamente a la elaboración del mapa de riesgos.

Un primer paso necesario para elaborar un mapa de riesgo es establecer y definir las escalas que se utilizarán para determinar la INTENSIDAD y FRECUENCIA de cada riesgo analizado. En este documento utilizaremos las siguientes:

IMPACTO	
MODERADO	Las consecuencias obligan a modificar algunos medios o procesos causando perturbaciones económicas asumibles en los resultados anuales. En caso de producirse daños reputacionales, serían puntuales y sin impacto mediático.
RELEVANTE	Las pérdidas originan dificultades considerables en el corto plazo obligando a modificar algunos objetivos con repercusión en los resultados anuales. Ejemplos: i) daño menor en los activos de la organización, ii) incumplimiento formal de alguna ley o regulación que puede ser subsanado, iii) causar un perjuicio menor a un individuo, que -aunque sea molesto- puede ser subsanado, iv) daños reputacionales apreciables, pero reparables, con eco mediático, v) daños en la percepción de los clientes que puedan dar lugar a una ligera pérdida de estos vi) daños en la relación con proveedores que puedan dar lugar a ligeras cancelaciones o peores condiciones en los contratos.
GRAVE	Su impacto es tal en los resultados que obliga a reconsiderar no solo el corto plazo sino también los planes de futuro de la organización. Ejemplos: i) reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones, aunque estas sigan desempeñándose ii) sufrimiento de un daño significativo de los activos de la organización iii) incumplimiento

material de alguna ley o regulación que no tenga carácter subsanable iv) causar un perjuicio significativo a un individuo de difícil reparación v) daños reputacionales elevados, de difícil reparación, con cobertura en medios de comunicación nacionales vi) daños en la percepción de los clientes que puedan dar lugar a una importante pérdida de estos vi) daños en la relación con proveedores que puedan dar lugar a significativas cancelaciones o peores condiciones en los contratos.

CATASTRÓFICA Amenazan la propia supervivencia de la organización.

Ejemplos: i) la anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales ii) el daño muy grave, e incluso irreparable para alguno de los activos de la organización iii) incumplimiento grave de alguna ley o regulación iv) causar un perjuicio grave a algún individuo, de difícil o imposible reparación v) daños reputacionales muy elevados, de difícil reparación, y cobertura continua en medios de comunicación nacionales e internacionales vi) daños en la percepción de los clientes que puedan dar lugar a una drástica pérdida de estos vii) daños en la relación con proveedores que puedan dar lugar a grandes dificultades para continuar o establecer nuevos contratos.

Para valorar la intensidad desde un punto de vista económico se establecerán una serie de rangos, que serán función de las características del negocio.

PROBABILIDAD

REMOTA Si sucede de forma extraordinaria (una vez en el siglo o durante toda la existencia de la organización).

INUSUAL Si acontece rara vez (una vez cada 10 años).

OCASIONAL Si tiene lugar varias veces en un decenio.

FRECUENTE Si ocurre varias veces todos los años.

Si asignamos un punto al valor más bajo de la escala, dos al segundo más bajo, tres al siguiente, y cuatro al mayor, se elabora una matriz con la PROBABILIDAD y el IMPACTO, obteniendo el siguiente resultado al sumar los valores obtenidos tras la intersección de cada valor:

Matriz IMPACTO / PROBABILIDAD

IMPACTO \ PROBABILIDAD	REMOTA	INUSUAL	OCASIONAL	FRECUENTE
CATASTRÓFICA	5	6	7	8
GRAVE	4	5	6	7
RELEVANTE	3	4	5	6
MODERADA	2	3	4	5

Podemos clasificar como riesgo bajo aquellos que tengan una puntuación igual o menor que 3, riesgo alto los que tengan una puntuación mayor o igual a 6 y riesgo medio el resto.

De esta clasificación podemos establecer políticas generales para gestionar estos riesgos:

IMPACTO \ PROBABILIDAD	BAJA	**ALTA**
ALTA	**Riesgos excepcionales** Atenuar con seguros	**Riesgos preocupantes** Tratar con urgencia
BAJA	**Riesgos menores** Asumir	**Riesgos recurrentes** Prevención, controles, capacitación, sistemas...

Las posibles respuestas a los riesgos identificados, basándose en la norma ISO 31000, son:

1. Supresión del riesgo: aunque no es lo más habitual, a veces las organizaciones logran que desaparezcan los riesgos asociados a sus procesos. Esto es posible cuando la previsión se ha realizado de forma exitosa obteniendo información adicional, adquiriendo apoyo de expertos, añadiendo recursos adicionales o modificando los elementos de la planificación, entre otros elementos. En ocasiones una organización podría decidir abandonar algún tipo de actividad.

2. Transferencia del riesgo: el riesgo es transferido a otra dependencia de la organización o, incluso a una segunda empresa asociada, siendo este un recurso muy frecuente entre grupos de compañías filiales o que tienen en común algún tipo de vínculo que hace posible esta transferencia. Otra vía habitual es la de transferir un riesgo a una compañía aseguradora.

3. Mitigación del riesgo: es una estrategia de gestión de riesgos que consiste en reducir la probabilidad o el impacto de un riesgo sobre la organización.

4. Explotación del riesgo: si el riesgo posee efectos positivos, se podría potenciar gracias a la designación de más personal cualificado, un mayor apoyo económico, o una adaptación a la planificación realizada al inicio.

5. Aceptación del riesgo: si se disponen de riesgos que no suponen mayores problemas para la consecución de los objetivos y que pueden convivir con la empresa. No obstante, esto implica la elaboración de un plan de contingencia para adaptar el riesgo a la actividad de la entidad.

3. RELACIÓN DE RIESGOS ANALIZADOS

Para seleccionar los riesgos TIC (Tecnología de la Información y Comunicaciones) se han valorado distintos modelos. Entre estos se ha seleccionado el **modelo EBA**, que contempla los riesgos típicos del sector banca. Los motivos que han dado lugar a esta decisión han sido fundamentalmente dos: el primero que los riesgos recogidos pueden considerarse riesgos universales, válidos para cualquier tipo de negocio, el segundo es que en esta relación hemos encontrado un número de riesgos equilibrado, ya que un número reducido podían hacer demasiado superficial este trabajo y un número elevado hacerlo demasiado complejo para los fines perseguidos.

Esta relación contempla riesgos de competencia de las áreas de seguridad informática y riesgos que no son competencia de estas.

Como en el análisis que vamos a realizar agruparemos los riesgos según la clasificación anterior, codificaremos los riesgos de acuerdo con esta clasificación: riesgos competencia de seguridad (contendrán una S) y riesgos que no son competencia de seguridad (contendrán una N). Al final de la denominación de cada riesgo figura la codificación que se utilizará en el resto del documento.

3.1 RIESGOS PARA LA DISPONIBILIDAD Y LA CONTINUIDAD TIC.

1.1. Gestión inadecuada de la capacidad (1N.1).

- Falta de recursos (por ejemplo, hardware, software, personal, proveedores de servicios) que puedan dar lugar a la imposibilidad de alcanzar el servicio que requiere las necesidades del negocio, interrupciones del sistema, degradación del servicio o errores operacionales.

1.2. Fallo de los sistemas TIC (1N.2).

- Pérdida de disponibilidad del sistema debida a fallos de hardware o software.

1.3. Planificación inadecuada de DRP (Plan de Recuperación de Desastres) y Continuidad TIC (1N.3).

- Fallos en las soluciones de continuidad y recuperación de desastres cuando se activan en respuesta a un incidente.

1.4. Ciberataques disruptivos o destructivos (1S.1).

Ataques con diferentes objetivos (activismo, chantaje…) que provocan una merma en la capacidad operativa de la organización. A pesar de que existen numerosos tipos de ataques, los más comunes son:

- Una sobrecarga en los sistemas y redes que impide el acceso a los servicios informáticos por usuarios legítimos.
- Los más conocidos son ataques de ransomware (malware o virus que cifran la información y ficheros de un sistema), que impiden el acceso a los datos e información almacenados en un sistema.

3.2 RIESGOS DE SEGURIDAD TIC.

2.1. Ciberataques y otros ataques externos basados en TIC (2S.1).

- Ataques ejecutados desde Internet o redes externas con diferentes propósitos utilizando una variedad de técnicas cuyo resultado es el control interno de los sistemas TIC.
- Ejecución fraudulenta de transacciones de pagos llevadas a cabo por hackers mediante la explotación de brechas de seguridad de los sistemas de pago.
- Ataques a las comunicaciones y conversaciones con el objetivo de recoger información para cometer fraudes.

2.2. Seguridad TIC Interna Inadecuada (2S.2).

- Obtención de accesos no autorizados a sistemas TIC críticos dentro de la organización con diferentes propósitos con una variedad de técnicas.
- Manipulación no autorizada de los sistemas TIC originada por la gestión inadecuada de los accesos a estos.

2.3. Seguridad TIC Física Inadecuada (2N.1).

- Robo de activos TIC a través del acceso físico, pérdida de activos y datos.
- Daño deliberado o accidental de los activos físicos TIC causados por ataques terroristas, accidentes o manipulación inadecuada por el personal de la organización o terceras partes.
- Protección física insuficiente contra desastres que pueden provocar la destrucción parcial o total de los sistemas y centro de datos.

3.3 RIESGOS POR EL CAMBIO DE TIC.

3.1. Controles inadecuados sobre el cambio o el desarrollo TIC (3N.1).

- Incidentes en software, en Sistemas de Información y Comunicación (information and communication technologies, ICT) y en datos causados por errores no detectados o que aparecen como resultado de un cambio (p.e. efectos imprevistos de un cambio o a la mala gestión de un cambio debido a la falta de testeo o prácticas de gestión del cambio impropias).

3.2. Arquitectura TIC Inadecuada (3N.2).

- Una débil gestión de la arquitectura de las TIC al diseñar, construir y mantener sistemas de TIC (por ejemplo, software, hardware, datos) puede llevar, con el tiempo, a sistemas de TIC complejos, difíciles, costosos y rígidos, que ya no están lo suficientemente alineados con las necesidades del negocio. Se quedan limitados en comparación con los requisitos reales de gestión de riesgos.

3.3. Gestión Inadecuada del Ciclo de Vida y Parcheado (3S.1).

- Fallos en el mantenimiento de un adecuado inventario de todos los activos TIC en combinación con una mala práctica de parcheado, podría provocar sistemas vulnerables y obsoletos.

3.4 RIESGOS PARA LA INTEGRIDAD DE LOS DATOS.

4.1. Procesado o Manejo Inadecuado de TIC (4N.1).

- Debido a errores o fallos en el sistema, la comunicación y/o la aplicación, o al proceso de extracción, transformación y carga de datos (ETL) ejecutado erróneamente, los datos pueden dañarse o perderse.

4.2. Diseño Inadecuado de los Controles de Validación de Datos en los Sistemas TIC (4S.1).

- Errores relacionados con la falta de controles para aceptar datos de entrada, transferencia de datos, procesado y salida de datos en los sistemas TIC (p.e. validación de datos de entrada, conciliación de información, etc.).

4.3. Control Inadecuado de los cambios a los Datos en Sistemas TIC en Producción (4N.2).

- Errores de datos implantados, debido a la falta de controles en la corrección y justificado por la naturaleza de datos ejecutados en la producción de sistemas TIC.

4.4. Diseño Inadecuado de Arquitectura, Flujos, Modelos o Diccionario de Datos (4N.3).

- Falta de consistencia entre arquitectura de datos, modelo de datos, flujo de datos, diccionario de datos…
- **NOTA:** *Este riesgo no será objeto de estudio. Se considera que la complejidad que implicaría explicarlo no aportaría nada al objeto de este documento.*

3.5 RIESGOS POR LA EXTERNALIZACIÓN TIC.

5.1. Resiliencia Inadecuada de Terceras Partes (5N.1).

- No disponibilidad de servicios TIC críticos subcontratados, servicios de telecomunicaciones y servicios públicos.
- Pérdida o corrupción de datos críticos/confidenciales encargados al proveedor de servicios.

5.2. Gobierno Inadecuado de la Externalización (5N.2).

- Degradación o fallos importantes del servicio debido a procesos ineficientes de preparación o control del proveedor de servicios subcontratado.
- Una gobernanza ineficaz de la contratación externa puede dar lugar a una falta de aptitudes y capacidades adecuadas para determinar, evaluar, mitigar y supervisar plenamente los riesgos de la TIC y puede limitar la capacidad operacional de las instituciones.

5.3. Seguridad Inadecuada de Terceras Partes (5S.1).

- Impacto de la piratería en los sistemas de los proveedores de servicios TIC o en los datos críticos o sensibles almacenados en estos.
- Accesos no autorizados del personal de proveedores de servicios TIC a datos críticos o sensibles almacenados en estos.

4. CASO I

HOTEL FAMILIAR

4.1.- DESCRICPIÓN DEL CASO.

La empresa Hotel El Torcal tiene un hotel en la ciudad de Antequera. Es un hotel de 25 habitaciones, en un antiguo edificio palaciego remodelado que entraría dentro de la categoría de hoteles con encanto. El hotel es gestionado por la familia del propietario siendo el trato hacia sus clientes familiar.

Aparte de los atractivos turísticos de Antequera, su ubicación, a menos de 1 hora y cuarto por autopista de Málaga, Granada y Córdoba, hace que sea un lugar atractivo para pasar unos cuantos días.

El hotel, entre semana, está ocupado fundamentalmente por extranjeros. Los fines de semana lo ocupan tanto extranjeros como españoles.

Los clientes encuentran el hotel fundamentalmente a través de la web, dentro de los portales de reservas hoteleras como Booking. El 90% de las reservas se generan por esta vía. El 10% restantes provienen de agencias que ofrecen un tour con alojamiento y paquetes de experiencias (tipo Smartbox). De forma residual se producen reservas directamente a través de la web del hotel o llamando por teléfono por parte de personas que tienen conocidos que se han alojado. La media diaria de personas que entran a consultar el hotel es de 400 a través de portales y 20 a través de la web del hotel.

La valoración que dan los usuarios de este hotel en los portales de reservas es muy buena, 9 sobre 10. Siendo consciente de la importancia de la valoración para que un cliente opte por seleccionar este hotel entre otras opciones, además de ofrecer un buen servicio, se siguen los comentarios realizados para agradecerlos en la mayoría de los casos e informar de las lecciones aprendidas en otros.

El hotel no dispone de servicio de cocina, pero tiene contratado un catering para servir desayunos, comidas y cenas. El cliente debe solicitar estos servicios de forma anticipada. También gestionan reservas, ofreciendo la posibilidad de realizar el Caminito del rey, que en muchos casos es uno de los principales motivos por el que los clientes se alojan el fin de semana. Así, la reserva de dicha actividad se ha de hacer con un periodo de antelación de al menos 24 h y a través de la página.

Una vez que el cliente realiza la reserva, el sistema de información del hotel envía un correo al cliente ofreciéndole estos servicios. El correo direcciona a una página del sistema de información del hotel donde se recogen sus peticiones, debiendo contratar estos servicios con al menos 24 horas de antelación.

El nivel de ocupación medio durante el fin se semana alcanza el 80%. Entre semana es del 50%. En los puentes y la Semana Santa se alcanza una ocupación muy cercana al 100%. Los extranjeros suponen el 70% de la ocupación del hotel.

Otra vía de ingresos son los eventos. Se organizan unas 20 bodas y comuniones al año, además de un par de congresos de empresas.

Se tiene constancia de que prácticamente todos los extranjeros solicitan el servicio de desayuno y cena, mientras que los españoles solicitan únicamente el desayuno.

La facturación anual del hotel es de 610.000 euros, de los que 430.000 euros corresponden a los ingresos por habitaciones, 110.000 por servicios de restauración y 70.000 por eventos.

El negocio se gestiona reduciendo a lo imprescindible el papel. Toda la información para gestionarlo se encuentra en los sistemas de información del hotel. En la información de los servidores del hotel se guardan datos personales de los clientes, así como de posibles acercamientos comerciales a potenciales grupos de interés. Las licencias de software de los distintos programas están vigentes y se actualizan periódicamente.

Los sistemas tienen controles lógicos y físicos de entrada a la información, así como un sistema antivirus en todos los ordenadores. El sistema de información que gestiona el negocio hotelero reside en el servidor ubicado en el propio hotel. El servidor tiene seguridad física y existen controles ambientales en la sala (temperatura, humedad...) así como sistema de detección contra incendios. Diariamente se hacen copias de seguridad que se almacenan en la vivienda del propietario. Existe un contrato de mantenimiento con una empresa que da soporte al software de gestión donde se definen unos niveles de servicio incluyendo penalizaciones y se definen las medidas a tomar en caso de incidentes graves. El proceso de actualización de parches es trimestral.

La aplicación que se utiliza para gestionar el negocio es un software muy utilizado en el sector y altamente testado. Las máquinas están correctamente dimensionadas y no se trata de un negocio que tenga previsto un crecimiento importante.

El hotel cuenta con un Sistema de Alimentación Ininterrumpida (SAI) al que están conectados los sistemas identificados como más críticos tales como los sistemas de seguridad, de incendios y emergencias y sistema informático. Dicho SAI proporcionaría una autonomía a estos sistemas de 60 minutos y además sirve de protección para el caso de picos de tensión en el suministro.
Dos días antes de la fecha de entrada en el hotel, el sistema de información carga una

noche de estancia en la tarjeta de crédito del cliente. El resto de la factura se abona al salir del hotel.

Los datos de la tarjeta de crédito se guardan (o no) en los archivos del hotel o se hace a través de una pasarela de pagos. No cumple normativa PCI-DSS.

La gestión de pedidos de los servicios de restauración se realiza con un sistema de información que se integra con el de la empresa de catering, al igual que la de las actividades turísticas.

La falta de disponibilidad de los sistemas para ofrecer en los portales de reservas la disponibilidad y precios de las habitaciones tiene varios efectos negativos: se pueden perder reservas, se puede perder posición en las listas frente a otros hoteles e incluso podría suponer la expulsión del portal.

APETITO AL RIESGO

La familia vive con el sueldo asignado por la gestión del hotel. Los beneficios los dedican a gastos extraordinarios (como comprar un coche nuevo, viajes a otros continentes, cambiar el mobiliario de su casa particular, etc.) o al ahorro. Aunque un año no generen beneficios, no consideran que la continuidad del negocio quedara en entredicho. Si las pérdidas impidiesen el pago de los gastos del hotel, considerarían el traspaso del negocio. Incidentes que supusiesen un coste anual de hasta 10.000 euros se consideraría moderado.

Para la familia propietaria un incidente con un impacto económico de más de 200.000 euros tendría la consideración de catastrófico (supondría la venta del hotel), grave se encontraría entre 100.000 y los 200.000 euros, relevante entre 10.000 y 100.000 euros y moderado menos de 10.000 euros.

	IMPACTO
MODERADO	< 10.000 €
RELEVANTE	10.000 - 100.000 €
GRAVE	100.000 - 200.000 €
CATASTRÓFICA	> 200.000€

4.2.- CONTEXTO CIBERATAQUES Y OTROS ATAQUES EXTERNOS EN EL SECTOR HOTELERO.

El sector de los hoteles está especialmente expuesto a los ataques externos incluidos en el presente riesgo por una especial diferencia que tienen frente a otros comercios o negocios, y es que los hoteles utilizan las pasarelas de pago por tarjeta como uno de los principales elementos dinamizadores del negocio. Ya sea para realizar el pago de los consumos de los huéspedes o como medio de garantía frente a las reservas realizadas por los clientes o los consumos realizados en los hoteles por los clientes, los hoteles se encuentran en la necesidad de almacenar los datos de tarjeta [1] de los clientes en sus sistemas.

El presente escenario ha puesto en el foco de los cibercriminales el sector hotelero como uno de los sectores más atractivos sobre los que realizar ataques, con el principal objetivo de obtener los datos de tarjeta de los clientes. Otro factor que lo hace atractivo es la gran fragmentación que existe sobre el sector, por ejemplo en España de los casi 15.000 hoteles [2] que existen tan solo el 10% pertenece a grandes cadenas hoteleras[3] con más de 40 hoteles, lo que deja el 90% de los hoteles en pequeños empresarios que gestionan sus hoteles con sistemas fragmentados y locales en cada hotel, escenario que dificulta por una parte identificar escenarios de economía de escala que posibiliten la implantación de medidas de seguridad (tecnologías y servicios que suelen ser caros), o la aplicación de medidas de seguridad homogéneas para todos los sistemas.

Con este panorama, en el que se puede ver un sector con muchos actores de pequeño volumen que le dificulta el acceso a la implantación de controles de seguridad y un conjunto de activos que resultan valiosos (datos de tarjeta y datos de clientes) para los criminales, se puede concluir que es un sector con una alta exposición a los incidentes de seguridad por su alta rentabilidad para los atacantes.

4.3. ANÁLISIS DE RIESGOS.

4.3.1. RIESGOS QUE NO SON DE SEGURIDAD.

RIESGO 1N.1 (Gestión inadecuada de la capacidad).

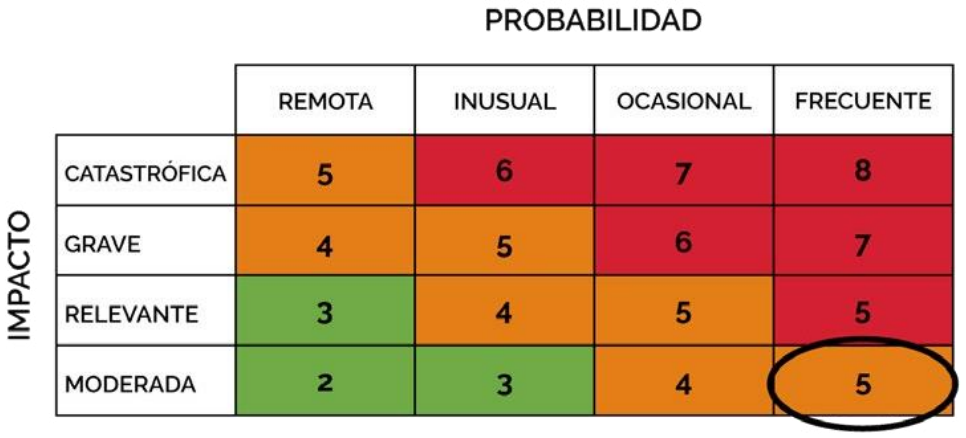
- El sistema de información impide la realización de reservas (paralización o excesiva lentitud). Incluso si el sistema fallase varios días de forma continuada, las pérdidas económicas podrían valorarse, manteniendo una proporción entre la media de ingresos diarios (1.700 euros) y los días sin servicio en una cantidad moderada (menos de 10.000 euros). No se considera que esta situación provoque una pér-

1 Datos de tarjeta mínimos para poder realizar un pago, número de tarjeta (PAN), fecha de caducidad, nombre del titular y código de seguridad (CVV)
2 https://es.statista.com/estadisticas/489035/establecimientos-hoteleros-abiertos-en-espana/
3 https://es.statista.com/estadisticas/502442/cadenas-hoteleras-espanolas-con-mayor-numero-de-establecimientos/

dida en la imagen de los clientes potenciales. La probabilidad la clasificaríamos como frecuente, al poder ocurrir varias veces al año.

- El sistema de información impide que el cliente pueda contratar servicios complementarios. En este caso, lo habitual sería que el cliente se dirija al hotel por teléfono, no teniendo un impacto en el negocio, aunque la probabilidad se clasifique como frecuente.

CLASIFICACIÓN DEL RIESGO.



RIESGO 1N.2 (Fallos de los sistemas TIC).

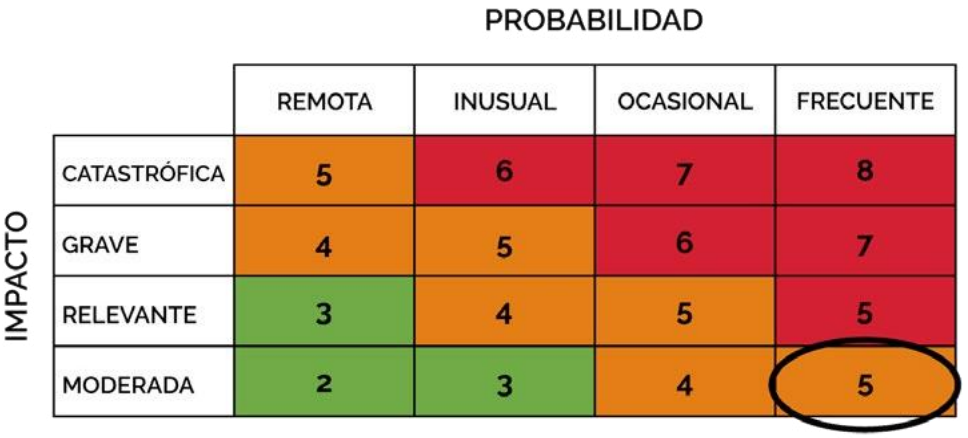
Aunque las causas de este riesgo son distintas a las relacionadas en el riesgo 1N.1, las consecuencias son similares.

Se añade una nueva causa de riesgo:

- El sistema de información opera incorrectamente. En este caso podrían producirse reclamaciones de clientes que de no solucionarse correctamente podrían incidir en las valoraciones publicadas en la web, reduciendo de forma drástica el número de clientes que pueden interesarse en contratar habitaciones. A modo de ejemplo podemos indicar aceptar reservas cuando no quedan habitaciones disponibles, no recoger solicitudes de clientes como las reservas de desayunos y cenas, reservas de actividades, etc. Habrá ocasiones en las que se pueda resolver el incidente contratando con urgencia el desayuno o cena y mejorándolo, ofreciendo otro hotel de la calidad superior incluso llegando a rebajar el precio de la reserva… Pero en otras no será posible (falta de disponibilidad de camas

en la ciudad en hoteles de cierta categoría, falta de entradas disponibles para visitar el Caminito del rey, etc.). Se considera que estos últimos casos serán muy poco frecuentes, y que con una buena y generosa gestión del incidente, los casos que puedan saltar a la red serán escasos, no afectando de forma apreciable la nota recibida por el hotel. El coste de atenciones especiales para resolver estas incidencias se podría aproximar a los 10.000€.

CLASIFICACIÓN DEL RIESGO.



RIESGO 1N.3 (Planificación inadecuada de DRP -Plan de Recuperación de Desastres- y Continuidad TIC).

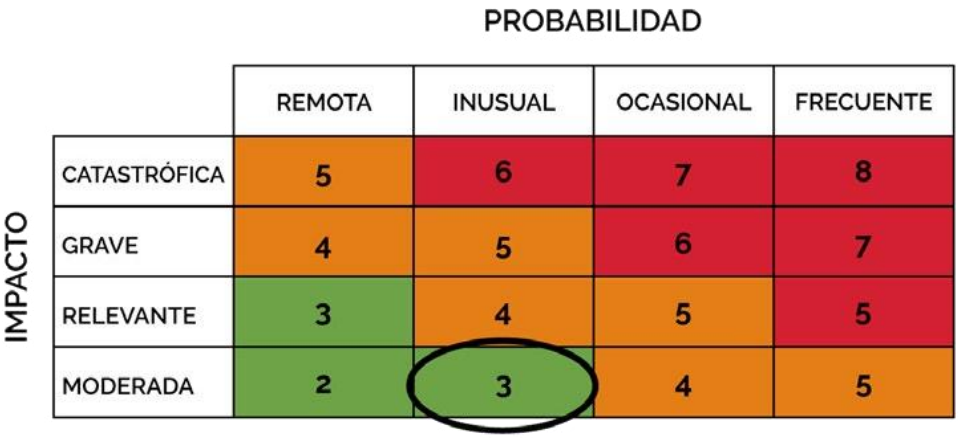
El Plan de Continuidad de Negocio persigue, tras identificar y analizar los posibles riesgos, el adoptar las medidas necesarias para garantizar que para cualquier contingencia que tenga lugar, haya definido un protocolo con el objetivo que la actividad se recupere lo antes posible minimizando así el impacto en el negocio. En este riesgo podemos centrarnos en evaluar dos condiciones: por un lado las personas, y por otro lado todo lo material relacionado con el servicio.

- En caso de que una persona dentro de la empresa posea un rol catalogado como crítico, habría funciones que podrían verse ralentizadas e incluso paralizadas. Por ejemplo, si únicamente existe un responsable de firma de contratos con proveedores, administrador de servidores, etc., y tiene lugar una contingencia, la entidad podría verse afectada por ello y no llevar a cabo funciones básicas, como pagar nóminas de empleados, pago a proveedores, adquisición de productos esenciales, etc…

- Si tuviésemos una caída del suministro eléctrico prolongado, esto además de afectar a los sistemas informáticos, comunicaciones, equipos de climatización, de presión de agua, neveras donde se almacenan los víveres, iluminación, etc. Ello ocasionaría reclamaciones y cancelaciones de los clientes.

- Si en el hotel hay contratado el servicio de catering con una empresa externa y esta por cualquier motivo quebrase o fuese paralizada su actividad por las autoridades sanitarias por una salmonelosis, por ejemplo. Esto haría que no se pudiese dar este servicio si no tenemos disponible otra alternativa.

CLASIFICACIÓN DEL RIESGO.



RIESGO 2N.1 (Seguridad física de la TIC inadecuada).

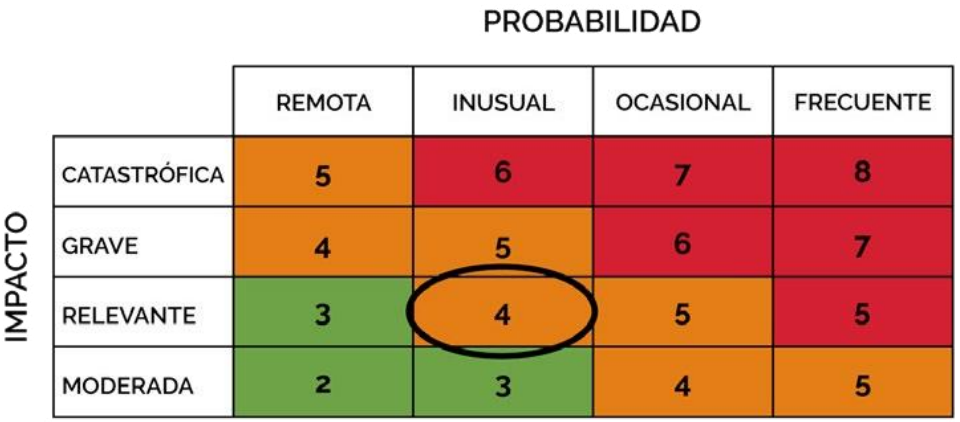
Este tipo de riesgo podría provocar las siguientes situaciones no deseadas:

- Robo o intrusión en el cuarto de servidores del hotel, lo que podría hacer que toda la parte del negocio que se gestiona mediante sistemas informáticos se quedase sin funcionamiento, tales como las reservas por Internet, consultas de clientes, etc. La duración de la incidencia iría en función del tiempo necesario para reponer la pérdida de activos y datos.

- Incendio parcial en el cuarto de servidores con afectación a los cables de conexión de comunicaciones, suministro eléctrico y SAI. Al tener copia de seguridad de la información diaria, la pérdida de información estaría limitada como máximo a las últimas 24 horas. No obstante, el restaurar de manera provisional los servicios dañados llevaría un tiempo durante el cual los sistemas informáticos y otros que se pudiesen encontrar en el mismo cuarto se verían afectados. Tales como las comunicaciones.

- Daño en un servidor por caída de líquido en su interior, debido a un accidente originado por un empleado del mismo hotel de manera fortuita. Lo que origina que las funcionalidades de dicho servidor se pierdan mientras se repara o se repone el mismo.

CLASIFICACIÓN DEL RIESGO.



RIESGO 3N.1 (Controles inadecuados sobre el cambio o del desarrollo TIC).

Un proceso de control de cambios que no logre establecer normas y procedimientos para las propuestas de cambio y satisfacer las necesidades de la Organización puede poner en peligro la integridad de los datos y las necesidades del sistema o de los usuarios de negocio. Si los procedimientos adoptados para la implementación del cambio no son eficaces, se podrían dar los mismos riesgos que si no existen. No adoptar procedimientos sistemáticos o respetar los existentes para iniciar las solicitudes de cambio, pruebas, documentar cambios, y autorizar cambios en los sistemas y procesos antes de la implementación puede resultar en cambios no exitosos. Además, la incapacidad para rastrear donde se habían hecho cambios podría retrasar la corrección de cualquier problema o incluso agravarlo. Este tipo de riesgo podría provocar las siguientes situaciones no deseadas:

- Los errores o fallos en la gestión de los cambios en los sistemas de información pueden suponer daños en los datos alojados en los servidores del hotel, así como en sus aplicaciones utilizadas provocando potenciales errores en la gestión de las reservas. Hasta la detección y corrección del fallo, las pérdidas económicas podrían valorarse, manteniendo una proporción moderada (menos de 10.000 euros). Si la subsanación del fallo no se realizara en un tiempo prudencial (1 mes), podría provocarse un impacto reputacional de los clientes potenciales. La frecuencia la clasificaríamos como frecuente.

- Los errores o fallos en la gestión del cambio en las comunicaciones (externas o internas) pueden impedir la prestación del servicio de reservas online (90% del total) y telefónicas, así como la generación de errores en las facturaciones a clientes, los pagos, incluso la correcta generación de copias de seguridad que podría

provocar futuras discrepancias en la información acumulada del negocio. Podría considerarse el riesgo como inusual y de intensidad relevante.

- Los errores o fallos en la gestión de los cambios en las aplicaciones podrían generar una alteración de los datos de terceros hasta la implementación de la actualización correspondiente del proveedor de SW. Se considera un riesgo inusual, aunque relevante por el impacto en terceros.

- Adicionalmente a cada análisis anterior, se incluirían las pérdidas de clientes y potenciales reclamaciones de estos, además de las sanciones regulatorias si hubiera alteraciones en los datos personales. Este impacto podría ser relevante por sus cuantías, especialmente por las sanciones de las AEPD, entre leves y graves (hasta el 2 % de la facturación: 12.200€) pero inusual.

CLASIFICACIÓN DEL RIESGO.

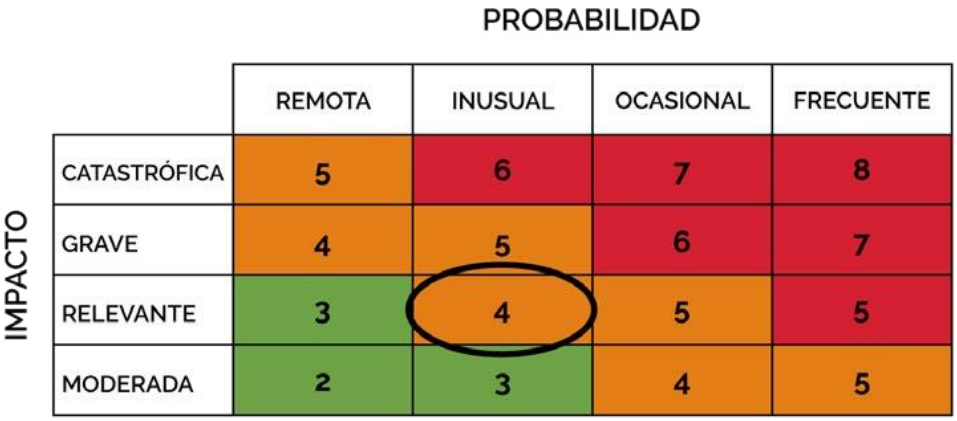
IMPACTO \ PROBABILIDAD	REMOTA	INUSUAL	OCASIONAL	FRECUENTE
CATASTRÓFICA	5	6	7	8
GRAVE	4	5	6	7
RELEVANTE	3	4	5	5
MODERADA	2	3	4	5

RIESGO 3N.2 (Arquitectura TIC inadecuada)

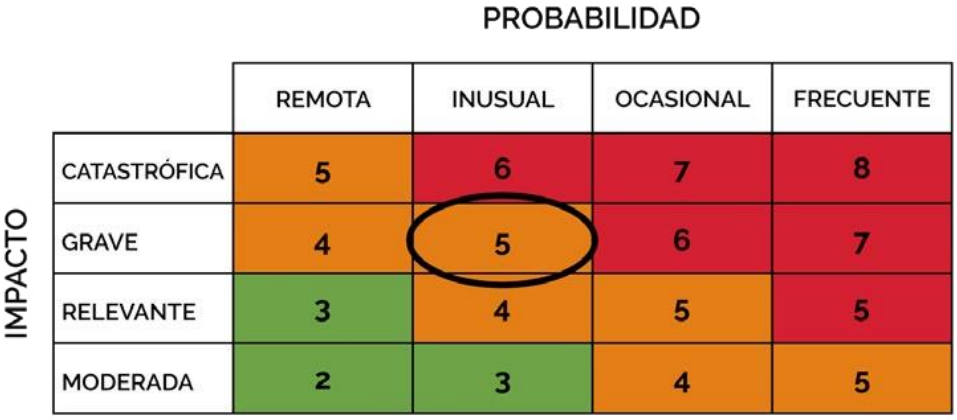
El diseño de la arquitectura que no incorpora o no permite incorporar entornos técnicos avanzados para el desarrollo o la mejora de aplicaciones en el futuro puede llevar a obstaculizar las perspectivas futuras de crecimiento de la Organización y exponerla a una falta de control del riesgo extrema.

Este tipo de riesgo podría provocar las siguientes situaciones no deseadas:

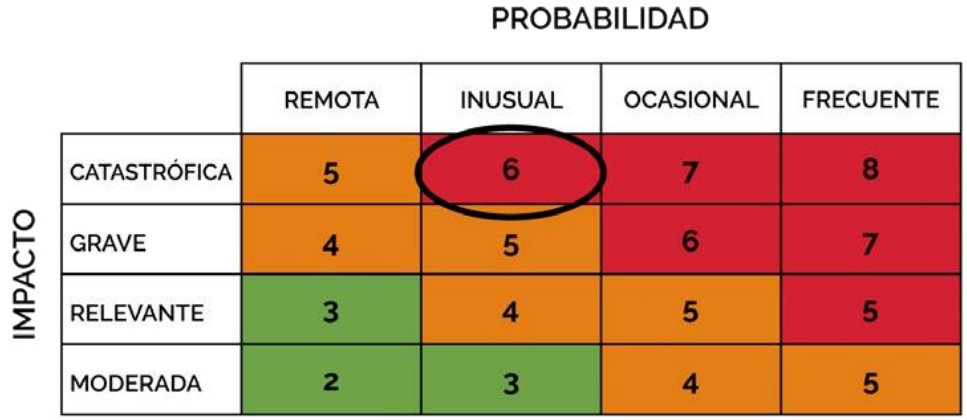
- La falta de adecuación a un negocio cambiante, hace que se puedan perder clientes por falta de acceso a la oferta del hotel o por no existir una base de datos suficientemente ágil para gestionarlos. Se da en una organización que no invierte en su negocio en tecnologías.



- En caso de no utilizar la tecnología adecuada la pérdida de capacidad de negocio para continuar existiendo tiene un impacto muy elevado, incluso el cierre del negocio. Se da en una organización que no invierte en su negocio en tecnologías.



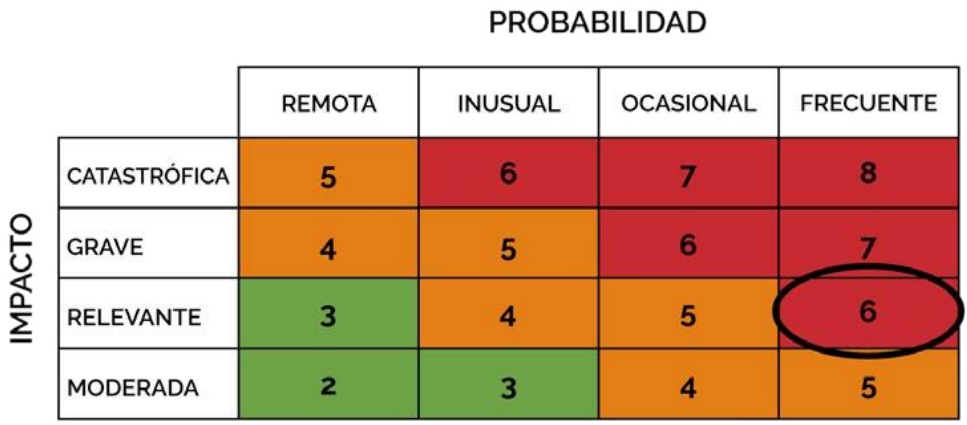
CLASIFICACIÓN DEL RIESGO.



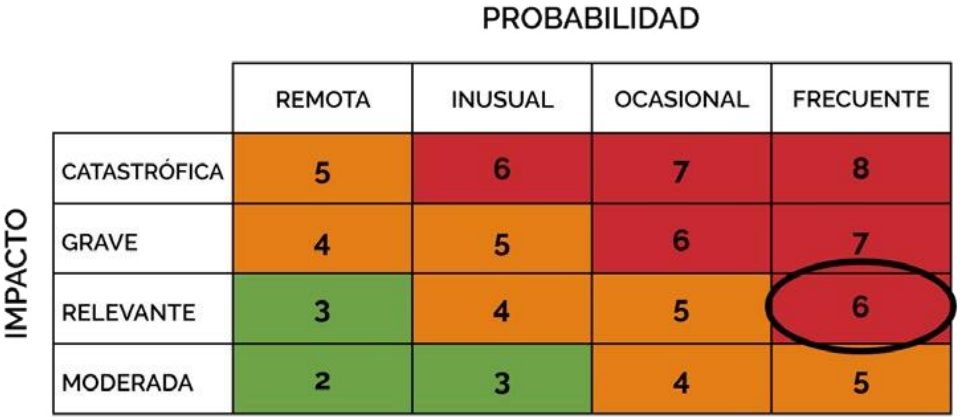
RIESGO 4N.1 (Procesado o manejo inadecuado de TIC).

Este tipo de riesgo podría provocar las siguientes situaciones no deseadas:

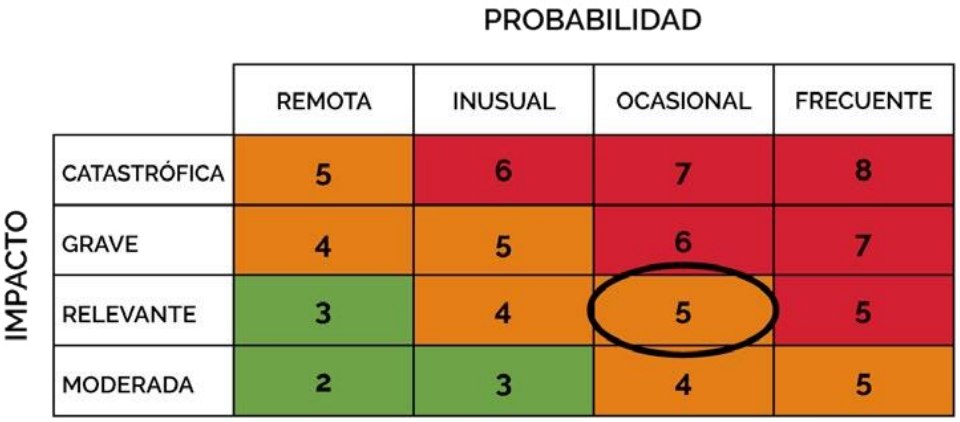
- Los errores o fallos en el sistema de información conllevan posibles daños en los datos alojados en los servidores del hotel, así como fallos en los procesos de las aplicaciones utilizadas provocando potenciales errores en la gestión de las reservas. Hasta la detección y corrección del fallo, las pérdidas económicas podrían valorarse, manteniendo una proporción entre la media de ingresos diarios (1.700 euros) y los días sin servicio en una cantidad moderada (menos de 10.000 euros). Si la subsanación del fallo no se realizara en un tiempo prudencial (1 mes), podría provocarse un impacto reputacional. La frecuencia la clasificaríamos como frecuente, al poder ocurrir varias veces al año.



- Los errores o fallos en las comunicaciones (externas o internas) pueden impedir la prestación del servicio de reservas online (90% del total) y telefónicas, así como la generación de errores en las facturaciones a clientes, los pagos, incluso la correcta generación de copias de seguridad que podría provocar futuras discrepancias en la información acumulada del negocio. Podría considerarse el riesgo como frecuente y de intensidad relevante.

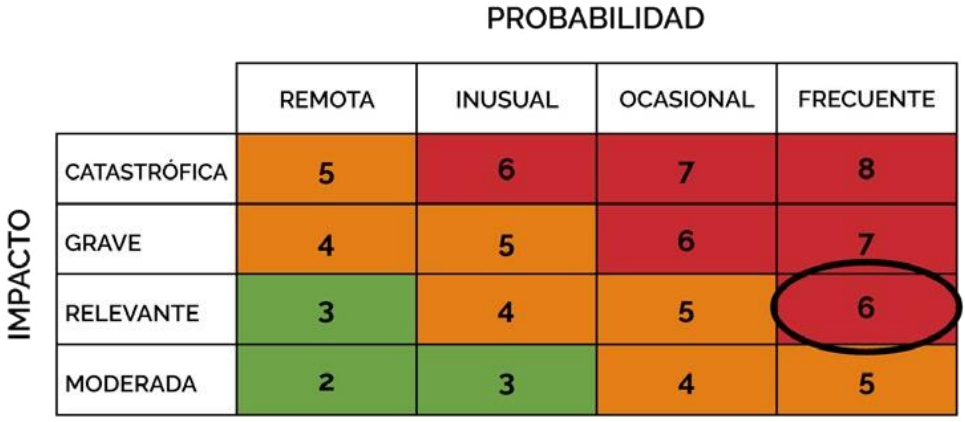


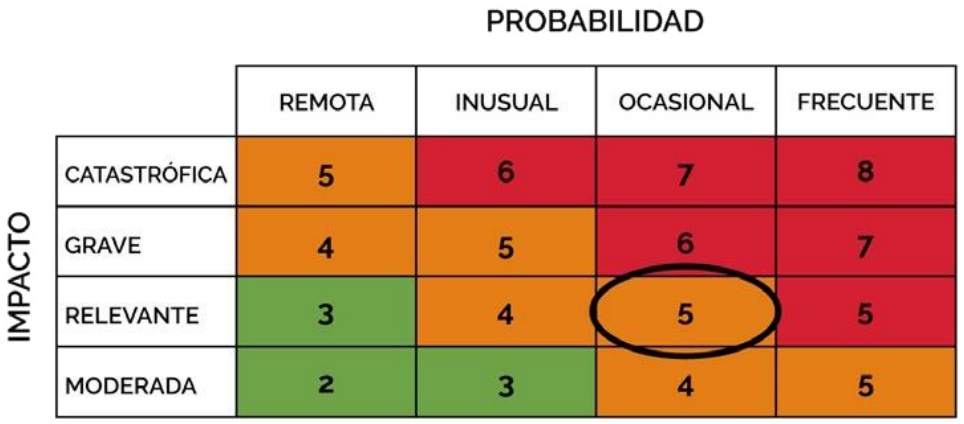
- Los errores o fallos en las aplicaciones, siendo estas estándar y mantenidas por sus fabricantes con los que se mantienen las correspondientes licencias vigentes y actualizadas, podrían generar una alteración de los datos de terceros hasta la implementación de la actualización correspondiente del proveedor de SW. Se considera un riesgo ocasional, aunque relevante por el impacto en terceros.



- Adicionalmente a cada análisis anterior, se incluirían las pérdidas de clientes y potenciales reclamaciones de estos, además de las sanciones regulatorias si hubiera

alteraciones en los datos personales. Este impacto podría ser relevante por sus cuantías, especialmente por las sanciones de las AEPD, entre leves y graves (hasta el 2 % de la facturación: 12.200€) pero ocasional.





CLASIFICACIÓN DEL RIESGO.

RIESGO 4N.2 (Control inadecuado de los cambios a los datos en sistemas TIC en producción).

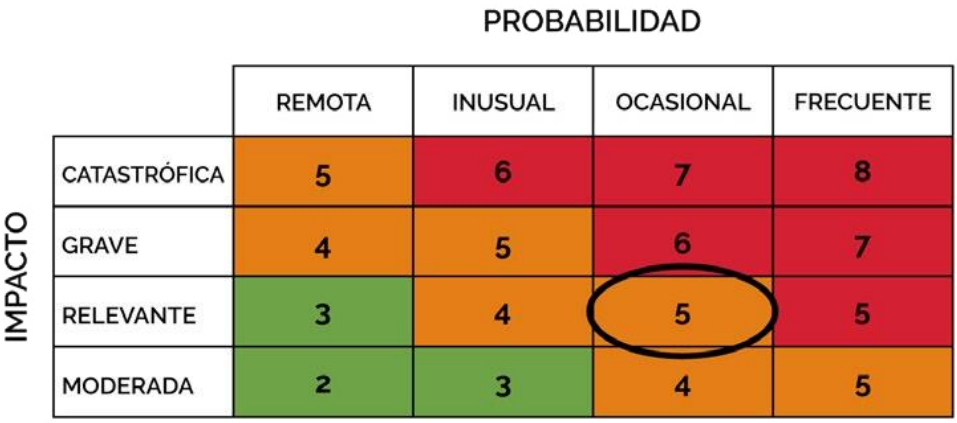
Este tipo de riesgo podría provocar las siguientes situaciones no deseadas:

- La falta de control de cambios en sistemas TIC, ocasiona que las modificaciones y actualizaciones requeridas sean gestionadas sin orden ni seguimiento adecuado, lo cual generará a medio/largo plazo la caída de sistemas que impediría la realización de reservas vía online. La gravedad de la situación será tan importante

como alineados estén los procesos de restauración de los sistemas, derivando en pérdidas importantes durante el periodo en cuestión, al recibir el 90% de las contrataciones vía on line.

- Habría que tener en cuenta un segundo impacto, precedido de la pérdida de datos por caída del sistema, donde el impacto en este caso se podría solventar en el caso de tener un backup adecuado, evitando pérdidas potenciales en el futuro de su base de clientes.
- Además, podrían producirse reclamaciones de terceros que han intentado modificar aspectos sobre lo contratado o servicios nuevos y no han llegado a materializarse por motivos ajenos al cliente.
- Cabe recordar que el impacto podría aminorarse si tenemos en cuenta que hay otras vías como la telefónica para poder solventarlo.
- La imagen se vería dañada, sobre todo por comentarios de terceros que hubieren sufrido percances.

CLASIFICACIÓN DEL RIESGO.



RIESGO 5N.1 (Resilencia inadecuada de terceras partes).

Este tipo de riesgo podría provocar las siguientes situaciones no deseadas:

- La resiliencia inadecuada ocasiona que tanto en el caso de problemas ocasionados en los sistemas TIC, así como en la pérdida de datos no ponga en marcha un proceso adecuado y urgente de restauración de sistemas y datos.
- La caída de los sistemas una vez más ocasionaría la imposibilidad de la gestión de reservas vía on line, así como la posibilidad de comunicación por esta vía para

cambios de última hora. Además de una pérdida de facturación durante el periodo, reclamaciones de terceros y pérdida de imagen, el no tener una correcta resiliencia, provocaría un mayor impacto en el negocio al verse prolongado el evento en el tiempo.

- Si además el problema se extiende a los servicios de telecomunicaciones y servicios públicos, el impacto podría derivar en que la empresa se quedara sin teléfono, así como sin energía, por lo que la indisponibilidad del servicio sería total, suponiendo un impacto del evento mucho mayor.

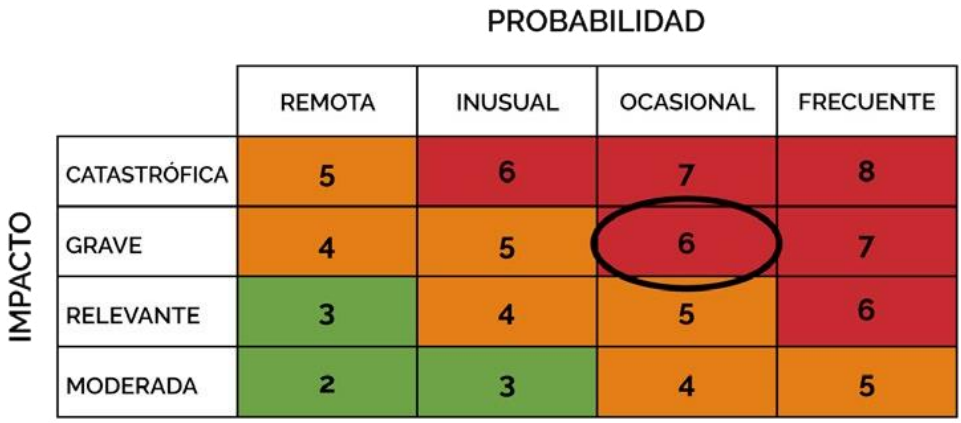
- Por otro lado, se debe tener en cuenta que la pérdida de datos confidenciales podría derivar en reclamaciones de terceros y del regulador, suponiendo impactos regulatorios, reputacionales y financieros.

- Otro aspecto a tener en cuenta es el acuerdo de responsabilidad que se firma en contrato con el proveedor (empresa subcontratada), ya que, aunque en un primer instante el perjuicio recae totalmente en el hotel, podríamos derivar responsabilidades al mismo. Igualmente, de cara a reclamaciones de terceros/regulador, podríamos actuar de la misma forma.

- La imagen se vería muy dañada.

- Es sumamente importante tener presente la resiliencia en cuanto a sistemas TIC.

CLASIFICACIÓN DEL RIESGO.



RIESGO 5N.2 (Gobierno inadecuado de la externalización).

Bajo la premisa de la necesaria existencia de un Gobierno Corporativo en todas las organizaciones, la diferencia de los riesgos tecnológicos frente a los riesgos tradicionales obliga a disponer de un modelo de Gobierno Corporativo de Ciberseguridad concreto que actuará como interfaz con cada función clave para determinar su exposición al ciberriesgo y establecer posibles planes de mitigación.

La ausencia o inadecuada gestión de los servicios IT externalizados impedirá disponer de los planes de mitigación de riesgos cibernéticos que incluyan las adecuadas inversiones en soluciones de ciberseguridad y seguros.

En este caso, la degradación o fallos importantes del servicio debido a procesos ineficientes de preparación o control del proveedor de servicios subcontratado, puede generar cualquiera de los riesgos de las anteriores naturalezas, en función del tipo de servicio que preste el proveedor. Por tanto, este riesgo será valorado en impacto como catastrófica de las que pueda identificarse en las anteriores, si bien la frecuencia la consideramos remota, al tener bien dimensionados los acuerdos con sus proveedores.

CLASIFICACIÓN DEL RIESGO.

IMPACTO \ PROBABILIDAD	REMOTA	INUSUAL	OCASIONAL	FRECUENTE
CATASTRÓFICA	5	6	7	8
GRAVE	4	5	6	7
RELEVANTE	3	4	5	5
MODERADA	2	3	4	5

4.3.1.- RIESGOS DE SEGURIDAD.

RIESGO 1S.1 (Ciberataques disruptivos o destructivos).

Dentro de este tipo de ataques, los más comunes que pueden sufrir un establecimiento del tipo del hotel son los de tipo de ransomware y que tendrían un impacto limitado en la operación del hotel, así como en su cuenta de resultados.

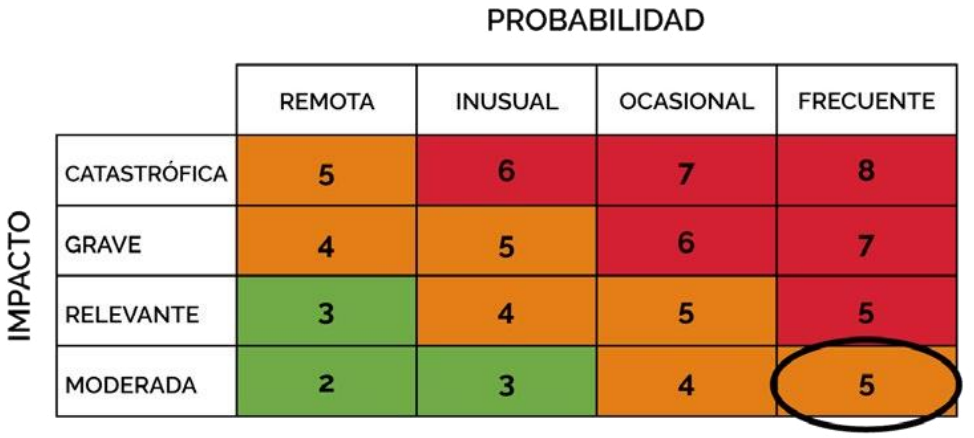
El auge y proliferación de los ataques de tipo de ransomware junto con su difícil detección, y unido al bajo nivel de protección que suele acompañar al conjunto de empresas tipo PyME, hacen que este tipo de ataques puedan considerarse como de tipo frecuente. Sin embargo, el impacto que puede tener en un hotel es limitado dado que el funcionamiento de este no se apoya en sistemas informatizados para la prestación de los servicios. Si bien, se podrían ver afectados los servicios de contratación, dado que el hotel depende en un 90% de las contrataciones web, no sería este su gran problema puesto que los grandes portales de contratación como Booking tienen grabados en sus sistemas las contrataciones realizadas por esta vía, y siempre sería posible recomponer la facturación. No obstante, el tiempo durante el que los sistemas del hotel no estuvieran disponibles no podrían responder a las peticiones de disponibilidad, por lo que durante este periodo de tiempo no se podría contratar.

Atendiendo a este razonamiento el coste medio esperado sería el siguiente:

Contratación web por día: (90% de 430.000€) 387.000€ / 365 1.060€ al día

Por lo que el coste máximo esperado no superaría los umbrales económicos de MODERADO

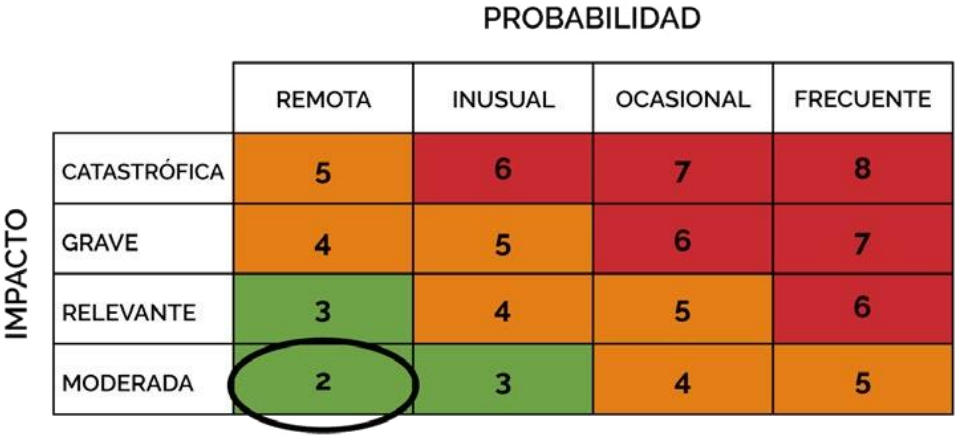
CLASIFICACIÓN DEL RIESGO.



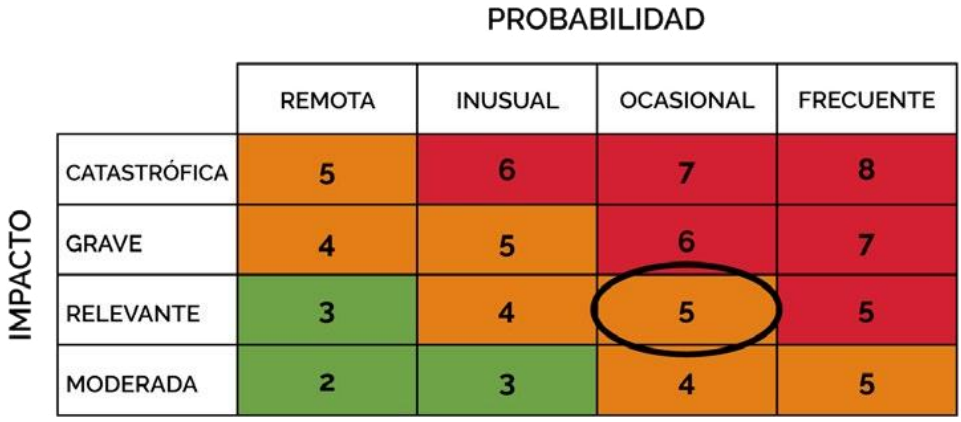
RIESGO 2S.1 (Ciberataques y otros ataques externos basados en TIC).

Desde un punto de vista de la gestión de riesgos, el nivel de los posibles escenarios de ataque e impacto a los que se expone el hotel son:

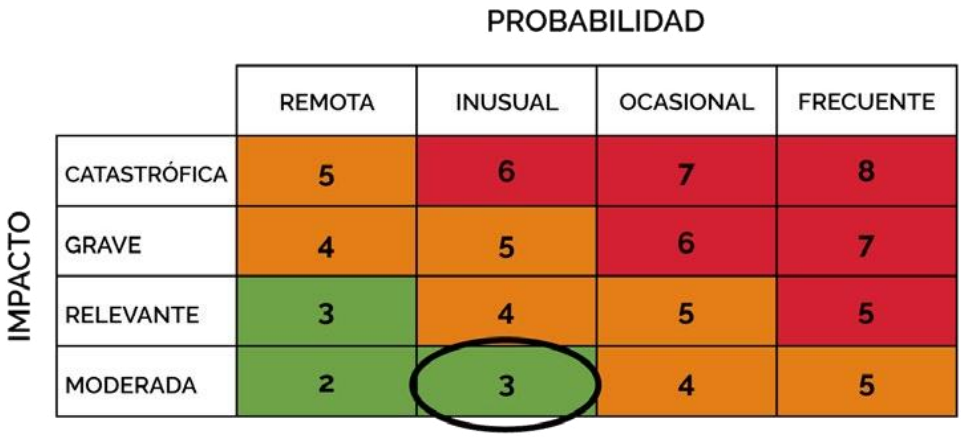
- **Ataques de fraude[4], espionaje, activismo social, sabotaje y ciber terrorismo.**
  Los actores que suelen estar detrás de este tipo de ataques no suelen tener entre sus objetivos los pequeños hoteles por el escaso impacto (fraude, activismo social, sabotaje, espionaje y ciber terrorismo) que puede tener. Por lo que la posibilidad de que ocurra es REMOTA y los efectos en cualquier caso muy limitados.



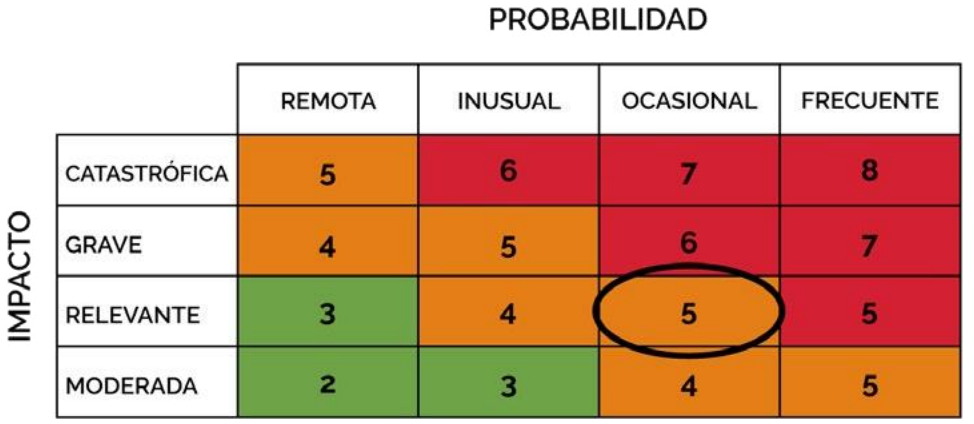
- **Ejecución de transacciones fraudulentas de pago (e-banking).**
  El ataque más plausible sería aquel en el que los delincuentes se hicieran con las claves bancarias del hotel y fueran capaces de desviar los fondos monetarios del hotel a otras cuentas bancarias. En este caso sí que la probabilidad de ocurrencia se puede clasificar como OCASIONAL (varias veces en un decenio) y el impacto económico directo como relevante, ya que difícilmente los fondos del hotel superarían los 60.000€ (casi 1/10 de la facturación). Además, hay que tener en cuenta que entrarían en juego los controles de los sistemas del banco que suelen establecer límites de transferencias, detección de transferencias inusuales, etc. Además, también habría que pensar en un posible efecto sobre la reputación del hotel, pero dado el tamaño y relevancia del mismo, se considera despreciable respecto al económico (dado que este impacto no afecta a los clientes).



- **Ataques a los sistemas de comunicación.**
  Este tipo de ataques vendría caracterizado por la interceptación de mensajes entre el hotel y los clientes o potenciales clientes. Dado que en el caso del hotel se produce una comunicación entre el hotel y los clientes, existe la posibilidad de que un delincuente que tenga acceso a esos datos de contacto de los clientes (potenciales, nuevos y ya existentes) pueda ofrecer servicios a muy buen precio a cambio del adelanto de una pequeña cantidad económica. Este tipo de ataques existen, pero en el sector hotelero son poco frecuentes y tienen un impacto muy limitado, por lo que la posibilidad del ataque se ha clasificado como INUSUAL y el impacto MODERADO.



CLASIFICACIÓN DEL RIESGO.



RIESGO 2S.2 (Seguridad TIC interna inadecuada).

Los daños que pueden derivarse si se materializa la amenaza están relacionados con la pérdida de confidencialidad, integridad y disponibilidad de la información y el impacto reputacional y/o económico para el hotel si trascienden las consecuencias.

Pormenorizando en cada uno de los riesgos particulares de este tipo de riesgos, podríamos enfrentarnos a las siguientes situaciones:

- **Obtención de acceso no autorizado a sistemas de TIC críticos** del hotel para diferentes propósitos (por ejemplo, fraude, realizar y ocultar actividades comerciales ilegales, robo de datos, activismo/sabotaje). Puede materializarse cuando se produce una sustracción/usurpación de credenciales, o se obtienen accesos y/o privilegios para los que no se está autorizado.

Esta amenaza se relaciona con los controles de acceso lógico a sistemas y aplicaciones, contando los sistemas de información del hotel con controles lógicos y físicos de entrada a la información, así como un sistema antivirus en todos los ordenadores, por tanto, cuenta con unos protocolos adecuados de seguridad los cuales han sido vulnerados.

Aunque la frecuencia pueda variar, existirían varios escenarios posibles en caso de materializarse el acceso no autorizado, dependiendo tanto del tipo de acceso conseguido (usuario de servicio de mantenimiento, usuarios del hotel, etc.) como del impacto, que podría ser grave debido a la virulencia de las acciones que podrían realizar los atacantes, dada la gran variedad de técnicas que podrían realizar, como robo de credenciales con el máximo privilegio en el sistema informático del hotel, que podrían explotar vulnerabili-

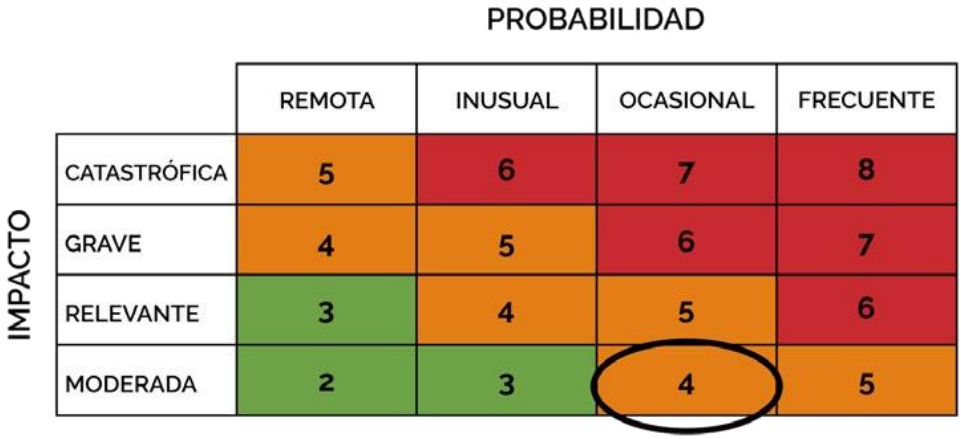
dades del sistema o desplegar software malicioso provocando la interrupción total del servicio, afectando a la casi totalidad de la actividad del negocio.

- **Caso de no disponibilidad del servicio.**

  La falta de disponibilidad de los sistemas, a pesar de que pueda tener efectos negativos, como pérdida de reservas, de posición en las listas frente a otros hoteles, e incluso podría suponer la expulsión del portal, una vez analizadas las consecuencias, el riesgo residual que queda no resulta tan alto, ya que atendiendo a la dependencia tecnológica que tiene el hotel, con el 90% de reservas se realizan a través de la web (ya sea por portales a los que da servicio, como a la propia página web del hotel), las pérdidas podrían llegar a ser cuantiosas. Atendiendo a los datos de facturación, se perdería el 90% de facturación de
  reservas de habitaciones, sumado al 100% de lo facturado en servicio de restauración, ya que solo se puede hacer uso mediante la web, hacen un total de 497.000 euros anuales, considerando las pérdidas como cuantiosas.

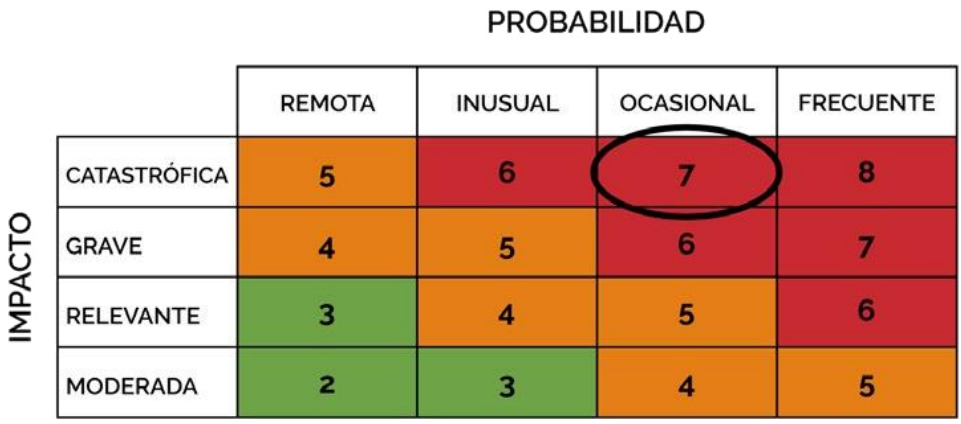
  Ahora bien, teniendo en cuenta las medidas de seguridad del hotel y de las personas que consultan la web a diario, repartiríamos esas cifras por días, y aplicando las medidas de seguridad instauradas en el hotel, como copias de seguridad en alojamientos externos a los sistemas de información, actualización de sistemas al día, con soporte de mantenimiento, con niveles de servicio definidos y una gestión ante incidentes graves, el riesgo residual que quedaría por la indisponibilidad del sistema informático durante dos días (tiempo necesario estimado para recuperar el sistema), supondrían unos 2.723,28 € (repartiendo la pérdida global de 497.00 € entre 365 días), a los que, además, habría que sumar 602,73 € por los servicios de restauración asociados. Así, se obtendría un impacto total de 3.326,01 € (bajo).

Este impacto estaría bastante mitigado debido a la existencia de copias de seguridad diaria, lo que contribuye a establecer un tiempo máximo de pérdida de información de 24 horas.



- **Caso de fuga de información.**

Especial atención merece este caso, en concreto en lo relativo a los datos de tarjetas de crédito que se almacenan en los sistemas informáticos del hotel, dado que, a pesar de disponer de pasarela de pagos, en la que se entiende que estos temas están debidamente ajustados desde el marco contractual establecido con la entidad bancaria suministradora del sistema de pago, en el propio hotel se almacenan datos de las tarjetas de crédito de los clientes como mínimo a modo de garantía de pago. Dado que el establecimiento no se ha declarado como cumplidor con la normativa aplicable en este tipo de transacciones, (PCI-DSS), la matriz resultante queda modificada, dado el elevado riesgo que se desprende de esta característica, siendo la siguiente:



Una fuga de información puede tener consecuencias nefastas para el hotel, por una parte, por mala publicidad, daños a su reputación, costos asociados al seguimiento de créditos con los clientes y demandas por parte de clientes afectados y sanciones por incumplimiento de normativas, por ejemplo, la de protección de datos aplicable en España, RGPD y LOPDGDD. Atendiendo solo a esta (las sanciones por incumplimiento de PCI-DSS no es directa y luego se abordará en un caso concreto), la sanción que le podrían imponer al hotel, correspondería a una conducta que incurriría en una sanción grave (falta de adopción de medidas técnicas y organizativas necesarias para la efectiva protección de datos), con multas que pueden ascender a una cuantía máxima del 2 % de la facturación, lo que en nuestro caso supone unos 12.200 €, impacto relevante según los rangos estudiados.

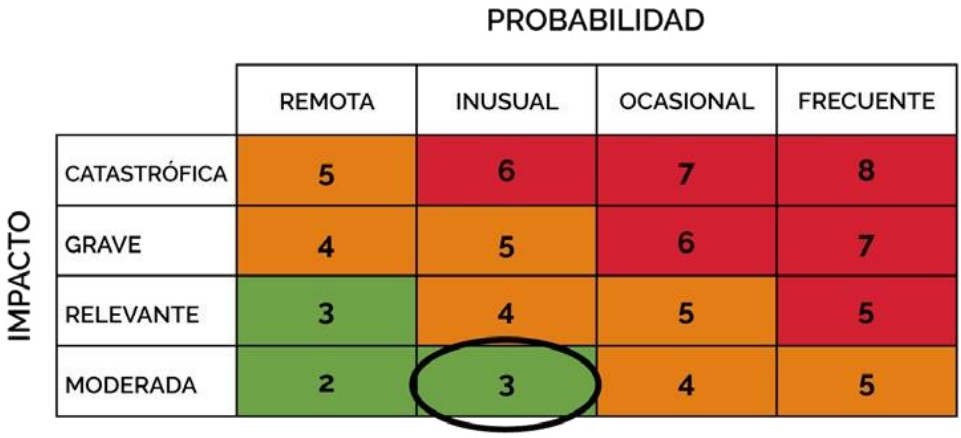
En este caso, la intensidad del ataque podría ser frecuente dado el índice de ocurrencia a nivel mundial que existe dentro de este sector, siendo el hotel una "presa fácil" al carecer de las medidas exigidas por la normativa PCI-DSS para el almacenamiento de datos de tarjetas de crédito. Sin embargo, la intensidad puede ser catastrófica en el caso de este tipo de información (datos de tarjetas de crédito).

Haciendo un análisis del potencial de acopia de datos que el hotel podría hacer en un año, atendiendo al número de habitaciones (25), y la ocupación media del hotel (70%) el número de huéspedes al año tomando un cliente tipo que se hospeda de media dos noches, resultaría 3.193 (25*0,70*365/2) clientes anuales. Suponiendo que le roban este volumen de datos al hotel, todos los costes derivados de este robo los tendría que asumir el hotel, y contrastando con los ratios y estimaciones mundialmente establecidos (coste medio de reemisión de tarjeta 30 euros, y media de gasto en transacciones fraudulentas 500 euros) ascenderían a un total de 1.788.500€ (191.625€ (30€ *3.193) más 1.596.875€ (500*3.193). Cantidad que deberá hacer frente el hotel, que podría quedar mitigada en el caso de la existencia de algún mecanismo de transferencia.

A esta situación de impacto catastrófico, habría que añadir otra adicional dado que existe la posibilidad de que la entidad bancaria le retirase la licencia para operar con tarjetas de crédito al no demostrar la debida diligencia, por lo que el hotel podría ver mermada notablemente la capacidad para poder seguir operando tras el incidente.

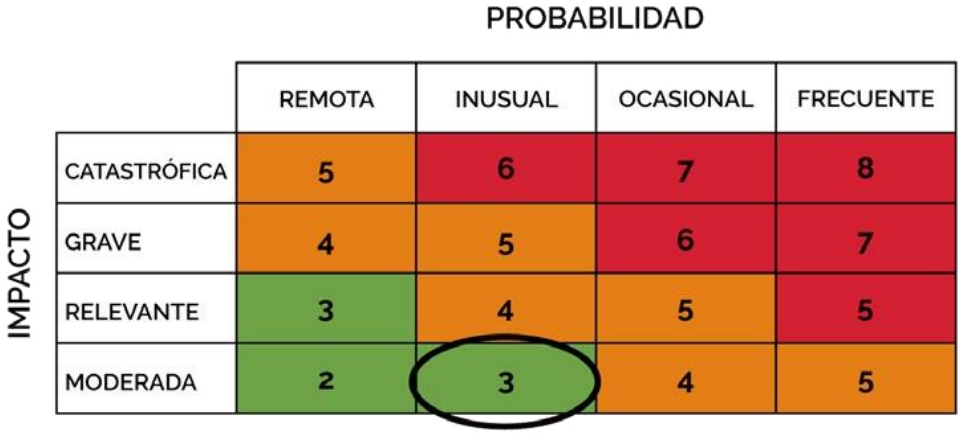
- **Manipulaciones no autorizadas de las TIC** debido a procedimientos y prácticas inadecuados de gestión de acceso a las TIC.
  Contando con las medidas de seguridad tanto lógicas como físicas establecidas para los sistemas de información del hotel alojados en el mismo, esta casuística resulta ser poco probable en el hotel, dado que la mayoría de los procesos están informatizados, realizados de manera automática por las aplicaciones de los portales web (pago por adelantado de la estancia, reserva de servicios, etc.…),

por lo que el usuario de la aplicación tiene poco margen de manipulación en los sistemas. En cuanto a la manipulación por parte de los usuarios de sistemas, está bien controlada debido al contrato de mantenimiento que tiene el hotel con la empresa que da soporte al software de gestión, definiendo penalizaciones en caso de anomalías, por lo que este tipo de situaciones deben estar perfectamente resueltas y procedimentadas para que no ocurran.

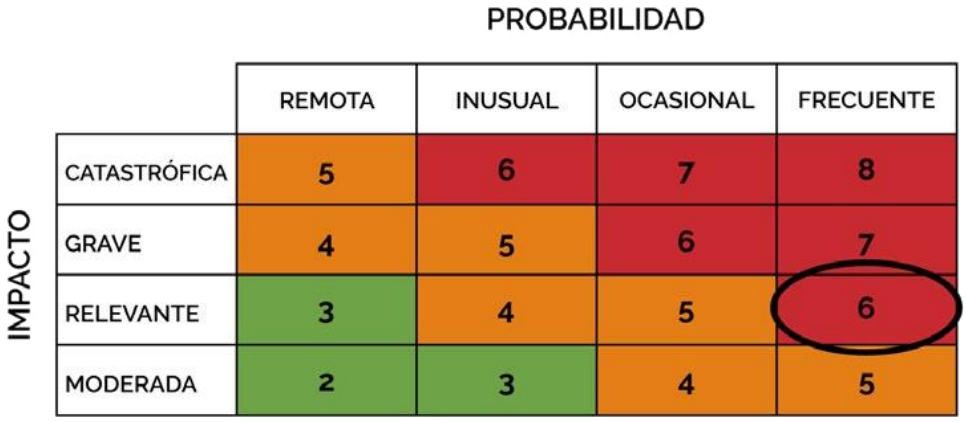


- **Amenazas de seguridad debido a la falta de conciencia de seguridad** por la cual los empleados no entienden, descuidan o no cumplen con las políticas y procedimientos de seguridad de las TIC.

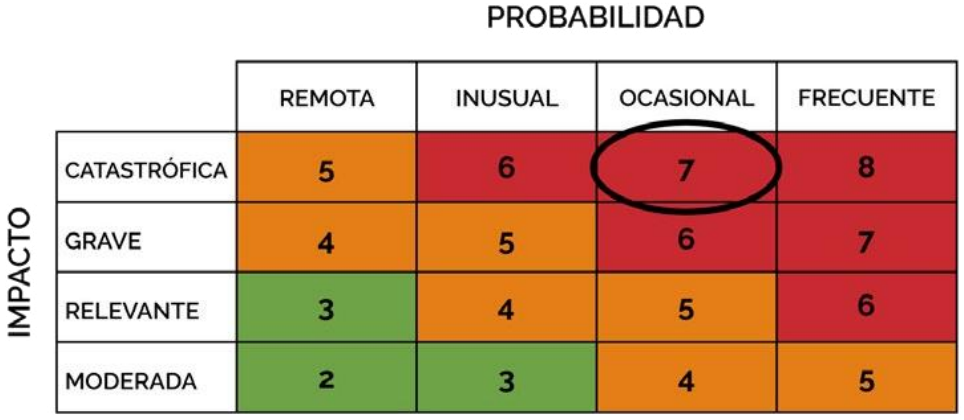
  Al igual que en el caso anterior, es poco probable debido a la poca interacción sobre procesos críticos de los usuarios normales del sistema, y la alta concienciación que debe existir en los usuarios de sistemas de la empresa contratada para el mantenimiento.



- **El almacenamiento no autorizado o la transferencia de información confidencial** fuera de la institución.
  Estamos en la misma situación que en caso de fuga de información, ya que las consecuencias son idénticas, se haya producido el incidente de manera intencionada o como consecuencia de un ataque. Esta particularidad sí tendría repercusión en las posibles reducciones de las sanciones impuestas y en caso de reclamaciones.



CLASIFICACIÓN DEL RIESGO.



RIESGO 3S.1 (Gestión inadecuada del ciclo de vida y parcheado).

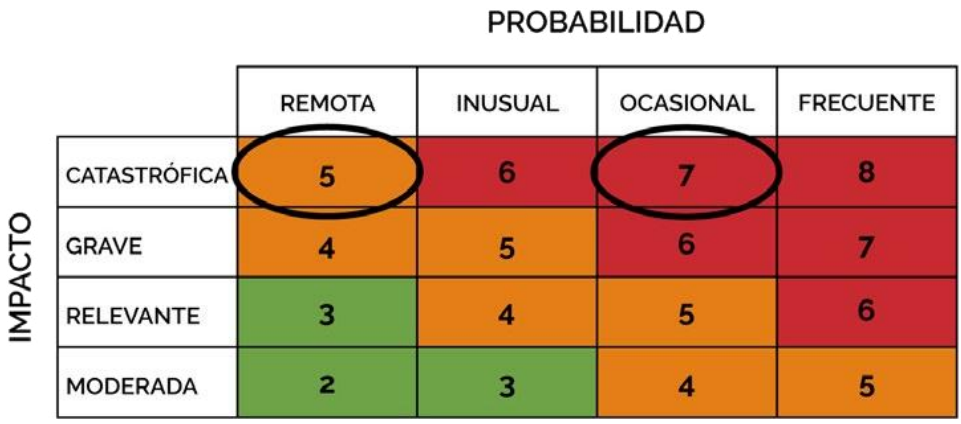
El presente riesgo tiene que ver realmente con el nivel de exposición de los sistemas con respecto a las diferentes vulnerabilidades que suelen aparecer durante el transcurso del ciclo de vida de los sistemas. Un sistema vulnerable por sí solo no supone ningún impacto para una empresa, pero lo cierto es que este tipo de escenarios de riesgo posibilitan el impacto de otros riesgos, en particular:

- 1S.1 Ciberataques disruptivos o destructivos.
- 2S.1 Ciberataques y otros ataques externos basados en TIC.
- 2S.2 Seguridad TIC interna inadecuada.

Por esto, el impacto se deberá enmarcar dentro del mayor de los riesgos anteriores, siendo el riesgo 2S.2 el más relevante a tener en cuenta para el caso de fuga de información, y dado el caso particular del hotel por el tipo de dato crítico que maneja (de tarjetas de crédito).

Para el cálculo de la probabilidad/frecuencia se puede tener en cuenta que lo más habitual es que todos los meses los fabricantes de SW publiquen sus boletines de seguridad en los que se incluyen los parches a instalar. Aunque no está especificado en el caso, lo más habitual es que en empresas maduras los ciclos de mantenimiento de SW estén comprendidos entre 1 y 6 meses, por lo que asumiendo una ventana de mantenimiento de 3 meses (sin tener en cuenta posibles incompatibilidades del software que utilice y que suele ser el principal impedimento para la actualización de los sistemas por dependencias entre estos), implicaría que durante este tiempo los sistemas del hotel serán vulnerables.

CLASIFICACIÓN DEL RIESGO.



El color rojo mostraría el riesgo al que se encuentra expuesto el hotel durante el periodo de tiempo de los 3 meses que los sistemas de este se encuentran desactualizados, y el naranja se correspondería con la ventana de tiempo en el que se actualizaría.

RIESGO 4S.1 (Diseño inadecuado de los controles de validación de datos en sistemas TIC).

El hotel dispone de una página web en la que potenciales clientes pueden hacer reservas, de hecho, según se indica en el caso, unos 20 potenciales clientes consultan todos los días

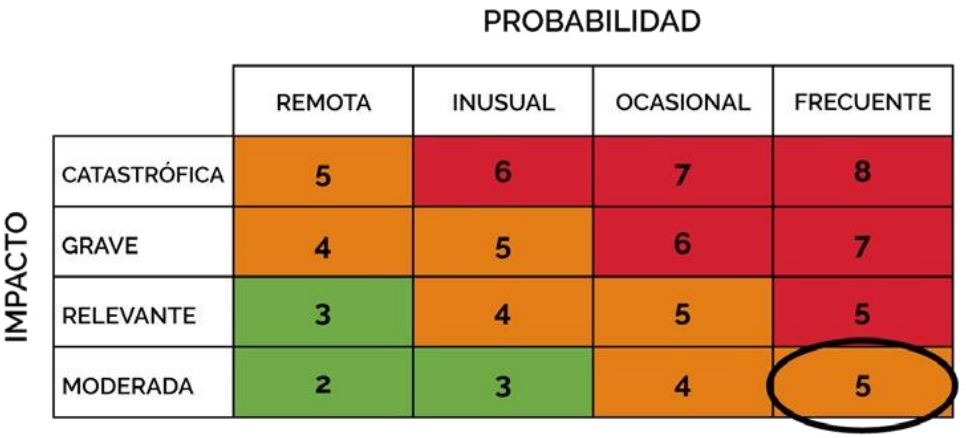
las páginas del hotel, pudiendo parecer relevante, aunque en realidad son apenas un 5% de las visitas que recibe el hotel, dado que la mayoría provienen de portales de mayoristas de contratación como Booking o similares. Por lo tanto, los principales datos de entrada en los sistemas del hotel serían la propia página web, así como las pasarelas de comunicación entre los portales mayoristas.

Respecto a los datos de salida, principalmente podemos identificar dos. El sistema de intercomunicación con la empresa de catering, que comunica con cierto tiempo de antelación los pedidos para los desayunos, comidas y cenas, y los sistemas bancarios para los pagos realizados por los clientes.

De las cuatro pasarelas de información, tan solo uno es un sistema operado por humanos (página web), siendo el resto pasarelas de información entre sistemas operadas entre sistemas automatizados. Esta distinción es relevante, dado que en los sistemas automatizados suelen existir tanto convenciones sobre el tipo de datos a introducir como operaciones de control de error que permiten un tratamiento de estos, por lo que con respecto a este riesgo se van a tratar de forma diferente.

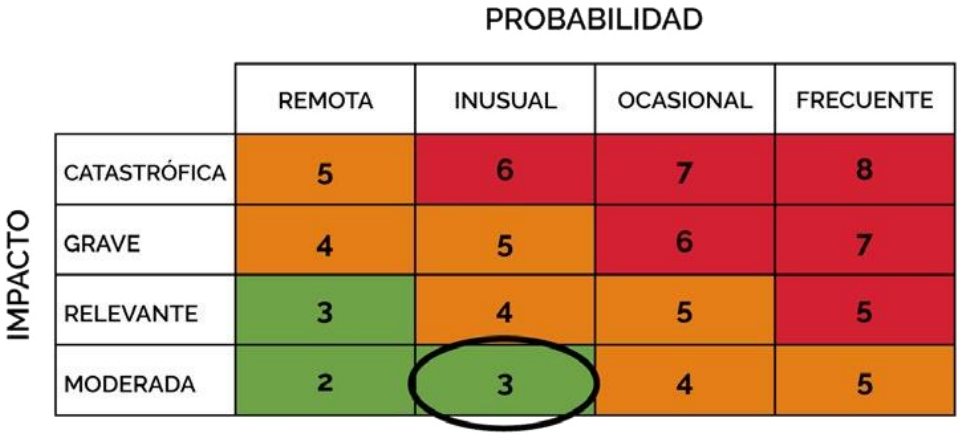
- **Página web.**

  La principal motivación que puede tener alguien para modificar los datos de entrada sería la de obtener bien un servicio por un precio inferior o incluso sin coste. Se trata de una ocurrencia bastante común, dado que no siempre hace falta tener unos conocimientos muy avanzados en informática para poder manipular los datos que se manejan a través de la página web, por lo que la posibilidad de que ocurra se ha clasificado en FRECUENTE. No obstante, el impacto que podría tener es muy limitado, ya que es difícil realizar un fraude a gran escala sin que pasara desapercibido por el personal del hotel.

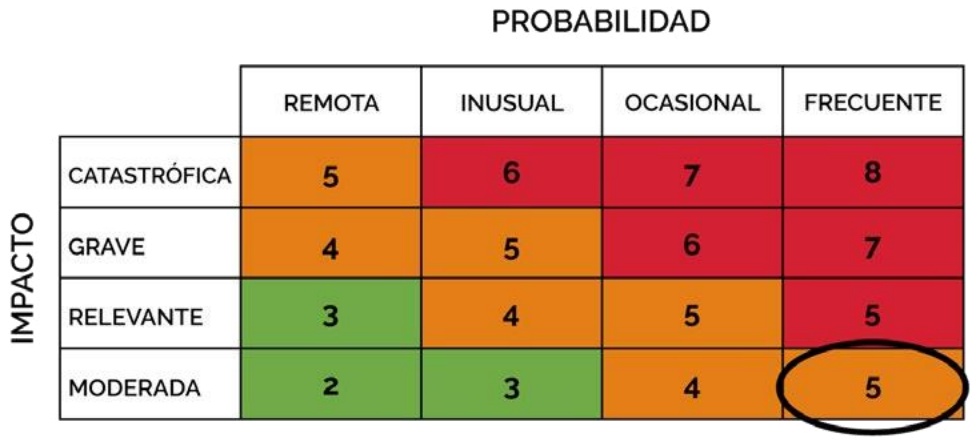


- **Portales de mayoristas, portal bancario, portal de proveedor catering.**

  En el caso de sistemas automatizados es difícil encontrar escenarios que puedan poner en riesgo al hotel, dado que cualquier impacto que pueda darse está limitado por dos factores: uno es que serán claramente evidentes en el funcionamiento del hotel (reservas, aprovisionamiento de catering, pagos o disponibilidad de efectivo) pudiéndose corregir en un espacio de tiempo muy pequeño.



CLASIFICACIÓN DEL RIESGO.



RIESGO 5S.1 (Seguridad inadecuada de terceras partes).

El hotel tiene varias terceras partes que infieren de manera directa sobre sus sistemas TIC:

- Empresa mantenedora sistemas informáticos.
- Entidad bancaria de pasarela de pagos.
- Conexión con plataformas de reservas turísticas.

- Entidad suministradora servicios restauración.
- Entidad suministradora productos turísticos.

Para todas estas empresas, los riesgos asociados a fallos debidos a una inadecuada seguridad estarían en parte relacionados con los distintos acuerdos establecidos con los mismos, y a la existencia de cláusulas especiales de transferencia de riesgos, como los seguros de ciberriesgos.

De manera general, habría que distinguir, además, del tipo de amenaza materializada en el tercero y el efecto directo en el hotel.

Se pueden distinguir varias casuísticas, en relación al grado de dependencia en los sistemas de información de las terceras partes y el hotel, alojamiento de servidores, nivel de intrusión en el sistema, etc.

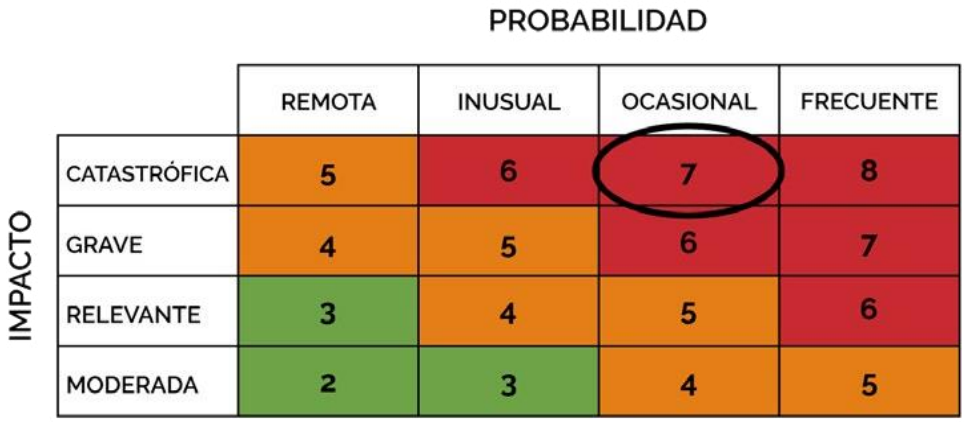
El riesgo común y directamente relacionado sería la falta de disponibilidad de los servicios dependientes de terceros debidos a una gestión inadecuada, y en todos estos estarían reflejados en los distintos acuerdos de servicio o (SLA´s) establecidos.

Profundizando en las causas, y trataríamos de excepcional el siguiente supuesto en el que el proveedor sí tiene interacción directa en las TIC del hotel:

- Tanto el hackeo de los sistemas TIC de la empresa contratada para el mantenimiento de sistemas, como el acceso no autorizado a los mismos por parte de su personal, podría afectar de manera directa en los servicios del hotel si tuviera almacenados datos en los servidores de este proveedor. Se descarta el estudio de este aspecto al no contemplarse como riesgo, por estar todos los sistemas de información alojados en servidores dentro del hotel, así como las copias de seguridad igualmente en otra ubicación distinta de las TIC del proveedor.

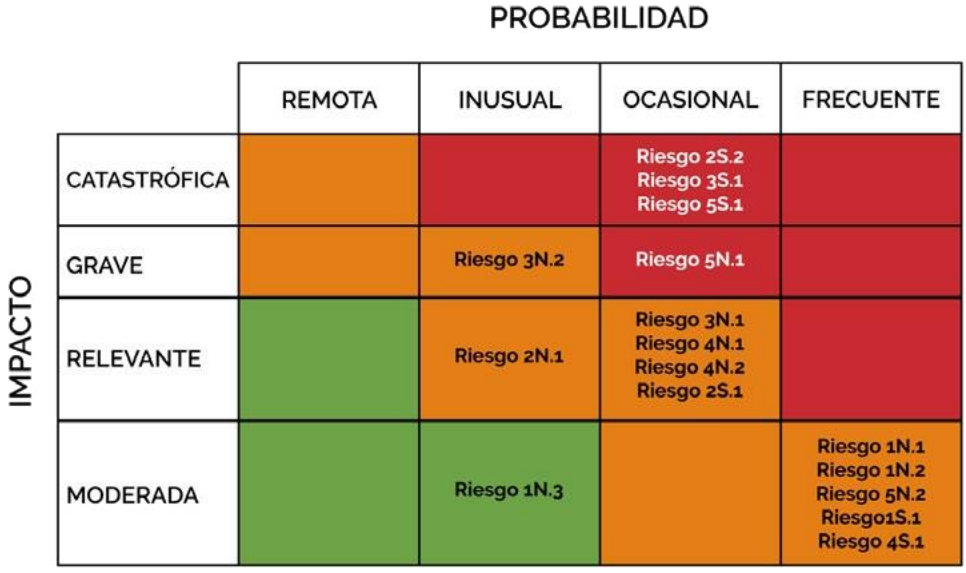
El único supuesto factible sería el robo de credenciales con permisos privilegiados con acceso a las TIC del hotel, para el mantenimiento contratado. Este aspecto ya ha sido tratado en el primer caso del punto:

RIESGO 2S.2: Seguridad TIC interna inadecuada.



4.4- MAPA DE RIESGOS.

A continuación, se representan todos los riesgos analizados en el mapa de riesgos.



Leyenda:

- RIESGO 1N.1 (Gestión inadecuada de la capacidad).
- RIESGO 1N.2 (Fallos de los sistemas TIC).

- RIESGO 1N.3 (Planificación inadecuada de DRP -Plan de Recuperación de Desastres- y Continuidad TIC).
- RIESGO 2N.1 (Seguridad física de la TIC inadecuada).
- RIESGO 3N.1 (Controles inadecuados sobre el cambio o del desarrollo TIC).
- RIESGO 3N.2 (Arquitectura TIC inadecuada).
- RIESGO 4N.1 (Procesado o manejo inadecuado de TIC).
- RIESGO 4N.2 (Control inadecuado de los cambios a los datos en sistemas TIC en producción).
- RIESGO 5N.1 (Resiliencia inadecuada de terceras partes).
- RIESGO 5N.2 (Gobierno inadecuado de la externalización).
- RIESGO 1S.1 (Ciberataques disruptivos o destructivos).
- RIESGO 2S.1 (Ciberataques y otros ataques externos basados en TIC).
- RIESGO 2S.2 (Seguridad TIC interna inadecuada).
- RIESGO 3S.1 (Gestión inadecuada del ciclo de vida y el parcheado).
- RIESGO 4S.1 (Diseño inadecuado de los controles de validación de datos en sistemas TIC).
- RIESGO 5S.1 (Seguridad inadecuada de Terceras Partes).

Este mapa nos permite priorizar la gestión para reducir el riesgo tecnológico. Aquellos riesgos que se encuentran en la zona superior derecha deben ser gestionados con urgencia, pues comprometen la supervivencia del negocio.

4.5.- ANÁLISIS DE RIESGOS CRÍTICOS – PLAN DE ACCIÓN.

Este apartado recoge planes de acción que permitirán reducir la intensidad y/o frecuencia de los dos riesgos más importantes detectados en el mapa de riesgos anterior. Se exponen dos a modo de ejemplo, ya pero que habría que desarrollar al menos planes para todos los riesgos que se encuentran en la zona ‘azul oscura’ del mapa.

PLAN DE ACCIÓN.

RIESGO 2S.2 (Seguridad TIC interna inadecuada).

El riesgo más evidente para el hotel viene por el potencial coste al que tendría hacer frente en caso de que un tercero pudiera robar los datos de tarjeta. El principal plan de acción sería el de hacer un plan de evaluación del grado de cumplimiento de la normativa PCI-DSS , en función del nº de transacción y volumen de las mismas, por una parte, y por otra, el modo en el que se realizan las transacciones. Así, el hotel, se podría enfrentar a dos procesos de cumplimiento de PCI diferentes:

Validación mediante un formulario de autoevaluación denominado SAQ (self assesment questionarie). De cara a cumplir con este proceso, existen diferentes guías a cumplimentar en función del tipo de almacenamiento y procesamiento de las tarjetas. Esta información se encuentra disponible en la web https://www.pcisecuritystandards.org/. En el caso de que el hotel requiera del almacenamiento del nº de tarjeta y el procesamiento de pagos sin la tarjeta física (utilizado muy frecuentemente como garantía de pago), estaría sujeto al formulario más extenso y exigente el tipo D (329 preguntas).

La otra opción sería que el Hotel adquiriera los servicios de un asesor cualificado (QSA – Qualified Security Assesors) que le guíe en el proceso de cumplimiento de PCI-DSS.

Con independencia de la fórmula a elegir, el Hotel estará sujeto a la realización periódica de un escáner de vulnerabilidades y test de intrusión, tanto interno y externo de los sistemas asociados, cuyo coste podría rondar entre los 1.000€ y 5.000€ en función de la complejidad de los mismos y de los sistemas a analizar. No obstante, lo más costoso en el caso de los sistemas sería la definición e implantación de un plan de seguridad lógica para aquellos sistemas que vayan a almacenar los números de tarjeta y todos aquellos que interactúen con ellos. Es difícil definir cuán costoso podría ser la definición y ejecución del plan dado que es necesario realizarlo en dos fases:

1. Levantamiento de información, del mapa de sistemas y definición del plan. El coste dado la simplicidad del esquema de sistemas de información del hotel, podría ser inferior a los 10.000€ (incluyendo la asesoría del QSA y los test de intrusión/análisis de vulnerabilidades iniciales).
2. Ejecución del plan de aislamiento y de fortificación de los sistemas de información incluidos en el esquema de certificación PCI-DSS. Esta fase es la compleja de determinar, ya que implica un conocimiento de detalle de bajo nivel, aunque sí que se puede establecer que es raro que exceda de los 50.000€ iniciales y de un máximo de 5.000-10.000€ anuales de mantenimiento, siempre que no se modifique el mapa de sistemas de información.

Aunque pueda parecer un coste no muy elevado, la otra opción que tendría el hotel sería la de buscar la contratación de un seguro que le diera cobertura económica para PCI-DSS ante una brecha de seguridad, aunque sería complicado que dada la facturación del hotel se pudieran encontrar capacidades superiores al millón de € que dieran cobertura a datos PCI-DSS. En este caso el coste de un ciberseguro suele estar rondando el 5% de la capacidad contratada por lo que la prima sería de unos 50.000€.

Es importante señalar que, aunque el seguro sería una opción, esta solo tendría una cobertura parcial del coste estimado, y adicionalmente solo tendría validez hasta la aparición del primer siniestro, dado que es raro que aseguradoras ofrezcan productos de aseguramiento cyber a entidades que muestren siniestros en repetidas ocasiones. El riesgo 5S.1 también estaría recogido dentro de este plan de acción dado que el máximo riesgo es el mismo que pueda ocasionar el del riesgo actual.

RIESGO 3S.1 (Gestión inadecuada del ciclo de vida y el parcheado).

El otro riesgo más significativo sería el relacionado con la seguridad inadecuada del ciclo de vida de los sistemas de información y del parcheado. Es importante señalar que dicho riesgo es relevante para el hotel, dado que puede acabar siendo la causa que materialice un ataque que acabe derivando en una brecha de seguridad, en su mayor pérdida para el hotel, que sería el caso de tarjetas de crédito. De hecho, lo más habitual es que este tipo de ataques se materialicen en entidades que manejan este tipo de información y la puerta de materialización sea la de aquellos sistemas de información que se encuentran expuestos en Internet y no estén debidamente actualizados ni fortificados.

En este caso lo más adecuado para el Hotel sería que contratara un servicio especial de mantenimiento de los sistemas de información que les garantice que los componentes y sistemas expuestos en Internet se actualizan periódicamente, estableciendo con el proveedor un periodo máximo de actualización de no más de 2 meses y siendo preferible que la ventana de actualización no supere el mes. Asimismo, el hotel deberá incluir dentro de este contrato de actualización de los sistemas aquellos casos denominados “Zero days”, que se corresponden con vulnerabilidades que aparecen en sistemas de información y son rápidamente utilizados por los cibercriminales para atacar los sistemas. Generalmente los fabricantes publican boletines de actualización de sus productos fuera de ciclo para que las entidades que utilicen dichos productos los instalen a la mayor brevedad.

Con lo anterior, se cumpliría el ámbito de la actualización de sistemas, no obstante, la configuración inadecuada de componentes también presenta el mismo riesgo y también debería incluirse en los servicios a incluir por el proveedor.

Ambos ámbitos deberán ser verificados periódicamente, para lo que se deberán incluir también servicios de escáner de vulnerabilidades y test periódicos sobre los sistemas informáticos del hotel. El coste es dependiente de la calidad y el alcance de los trabajos a implantar, pero podría estar comprendido entre los 3.000 y 10.000€.

Es importante señalar que tanto en el caso del riesgo 2S.2 y del riesgo 3S.1 se pueden dar situaciones de dificultad y coste añadidos, en particular en el caso de que las aplicaciones utilizadas por el hotel sean dependientes de una versión específica de software, sin que este pueda ser actualizado ya sea por dependencia o por obsolescencia. Estos costes son difíciles de estimar, dado que puede tener diferentes consideraciones como cambios en la aplicación, migración de la suite de aplicaciones a una versión superior (con cambio de licencia, componentes, etc.).

5. CASO II

VENTA WEB DE COMPONENTES DE TECNOLOGÍA

5.1. DESCRIPCIÓN DEL CASO.

La empresa Componentes de Tecnología S.A. se dedica a la venta de dispositivos de tecnología con un amplio espectro, desde componentes cotidianos para usuario final (TV, smartphones, consolas de videojuegos, etc.), componentes para usuarios avanzados (Tarjetas Gráficas, procesadores, etc.), hasta componentes para instaladores o empresas pequeñas (Routers, Switches, servidores, etc.). La estrategia de la empresa ha estado basada principalmente en la venta por el canal online, que le permite ofrecer precio competitivo gracias a unos márgenes de venta muy estrechos apoyado en unos costes operativos especialmente bajos.

La empresa se fundó a principios de la década del 2.000, con un enfoque radicalmente opuesto al actual. Los socios fundadores empezaron con una tienda de venta de componentes informáticos, y crecieron con el boom del PC Doméstico. Posteriormente, afrontaron un cambio de estrategia y apostaron por el canal de venta online (www.compotec.es). La empresa factura en la actualidad cerca de 300 millones de € y tiene 350 empleados distribuidos por sus 3 centros de trabajo (Madrid, Barcelona, Málaga).

La sede central está en la provincia de Málaga, en su centro de trabajo. Todas las sedes disponen de un amplio almacén y una tienda física. El almacén sirve tanto para albergar el material que tienen a la venta, como para la custodia de los pedidos que los clientes han realizado por Internet. En las tiendas físicas, los clientes pueden ir tanto a comprar directamente como a recoger sus pedidos. Como es lógico, todos los almacenes además sirven de centros logísticos para la distribución de pedidos, según las provincias que tengan asignadas estos. Ello implica disponer en todo momento y en tiempo real de un control exacto del stock de productos.

Con independencia de que es posible la venta de productos en sus tiendas físicas, la venta directa en las tiendas no supone más que un 10% de los ingresos por ventas totales, suponiendo tan solo un 30% de la actividad en tienda, dejando el resto para la entrega de pedidos realizados por Internet.

El 90% de los ingresos restantes provienen de su principal canal de venta, su página web. Anualmente se atienden casi 1 millón de pedidos, de sus más de 12.000 productos diferentes. El pico de pedidos en un día puede llegar a más de 50.000 pedidos (con actividad de más de 30 pedidos al minuto). A día de hoy la empresa supera ampliamente los 300.00 clientes registrados, para los que se ofrece distintas modalidades de pago como tarjeta de débito, transferencia bancaria y Paypal. Dado que la venta online es la más habitual, la empresa permite el pago rápido (y lo promueve) de sus pedidos mediante el

almacenamiento de los datos de pago del cliente, en la actualidad casi el 40% de los clientes disponen de dicha opción.

A pesar de la dura competencia (compite contra Amazon, MediaMarkt, El Corte Inglés, etc.) la compañía ha tenido un notable y sólido crecimiento basado en una serie de principios a los que se mantiene fiel:

- Tiempos de entrega en 2h en tienda o 24h en territorio nacional para el 95% de sus pedidos.
- Alto grado de satisfacción del cliente (95% de satisfacción de media).

Escenario que se refuerza con el más de un millón de clientes que tiene la compañía, y el alto grado de fidelidad de los mismos, dado que un 75% de los clientes repiten compra en el mismo año.

Los procesos críticos en los que sustenta la compañía son:

- Venta online – soportado por sistemas desarrollados por la propia compañía que le permite adaptar la web a las necesidades específicas de la organización. El sistema está conectado a los principales proveedores de pago para permitir el pago online de los pedidos, y tiene su propio módulo de gestión de clientes.

- Plataforma de logística – vinculado con su plataforma de venta online y con el control de stock en los almacenes. Permite ofrecer en tiempo real la disponibilidad de los productos a los clientes.

- Plataforma de logística: desarrollada también con tecnología propia, aunque apoyada en tecnología de terceros. Tiene una doble función, por una parte, conecta al departamento de gestión de pedidos con los proveedores de logística para la preparación y entrega de pedidos. Y, por otra parte, comunica a los proveedores de productos para el abastecimiento de productos sin stock o cerca de quedar sin stock.

- Canal de Atención al Cliente: producto de terceros, pero adaptado a las necesidades de la organización. Permite la gestión eficaz de las reclamaciones de clientes en un tiempo record. El departamento gestiona de media unas 400 llamadas y 1.000 emails y consultas vía RRSS, aunque se alcanzan picos de 1.000 llamadas y 1.500 emails.

Aunque no se trata de procesos tan críticos, también toman especial relevancia los siguientes procesos:

- Marketing: basado en canal online, vía anuncios en distintas plataformas de información (RRSS, periódicos, etc.), como en publicidad dirigida (buscadores, boletines de email, etc).

- Business Intelligence y CRM: el área de análisis de datos se encarga de anticipar posibles demandas de productos, así como de detectar problemas en la cadena de suministros que puedan amenazar los principios a los que la compañía se mantiene fiel.

- Gestión de proveedores: las relaciones con los proveedores, tanto suministradores de productos como de logística, también se considera un aspecto importante dentro de la cadena de suministro.

Con independencia de que gran parte del software utilizado por la compañía se ha desarrollado de forma interna, los sistemas de la empresa están ubicados en un Data Center de un tercero a cientos de km. de la empresa y además también tienen incorporados en su infraestructura de TI elementos en cloud ubicados en grandes proveedores.

APETITO AL RIESGO.

La empresa es propiedad de unos socios cuyo objetivo es hacer crecer el beneficio lo máximo posible a corto plazo para venderla a una de las grandes empresas de venta web. Un incidente que redujera de forma significativa el negocio podría provocar o un retraso en los planes de venta o una reducción importante del valor de venta.

Los socios consideran que un incidente por encima de los 2 millones de euros retrasaría los planes de venta, por lo que dan a este valor la consideración de grave.

Si el incidente provoca que se cierre un ejercicio con unas pérdidas superiores al beneficio del último ejercicio, el incidente sería catastrófico, ya que se considera que esta cantidad excede a la capacidad que tiene la empresa para conseguir prestamos. Teniendo en cuenta que el beneficio actual es de 3 MM de euros, un incidente con un coste superior a 6 MM de euros daría lugar a unas pérdidas de 3 MM de euros.

Se considera que 100.000 euros, podría ser una cantidad asumible. El rango relevante se establece entre los 100.000 y los 2 millones.

	IMPACTO
MODERADO	< 100.000 €
RELEVANTE	100.000 € - 2.000.000 €
GRAVE	2.000.000 € - 6.000.000 €
CATASTRÓFICA	> 6.000.000 €

5.2.- CONTEXTO CIBERATAQUES Y OTROS ATAQUES EXTERNOS EN EL SECTOR VENTA WEB.

Debido a su dependencia directa al funcionamiento de sistemas informáticos, consideramos este sector uno de los más expuestos a ciberataques y debido a esto uno de los más atractivos para cibercriminales.

Para el caso presente se considera la empresa un objetivo con alta exposición a ciberataques, debido a su amplia cartera de clientes (datos personales y tarjetas), además de presentar una plataforma de venta online y logística desarrollada internamente. Al no ser una empresa especializada en el desarrollo de este tipo de aplicaciones, consideramos sus niveles de seguridad bajos en comparación a sus competidores directos (Amazon, MediaMarkt, El Corte Inglés, etc). Este perjuicio puede llegar a ser catastrófico debido a que al menos el 70% de la actividad del negocio depende de estas aplicaciones.

5.3- ANÁLISIS DE CADA RIESGO.

5.3.1.- RIESGOS QUE NO SON DE SEGURIDAD.

RIESGO 1N.1 (Gestión inadecuada de la capacidad).

Este tipo de riesgo podría provocar las siguientes situaciones no deseadas:

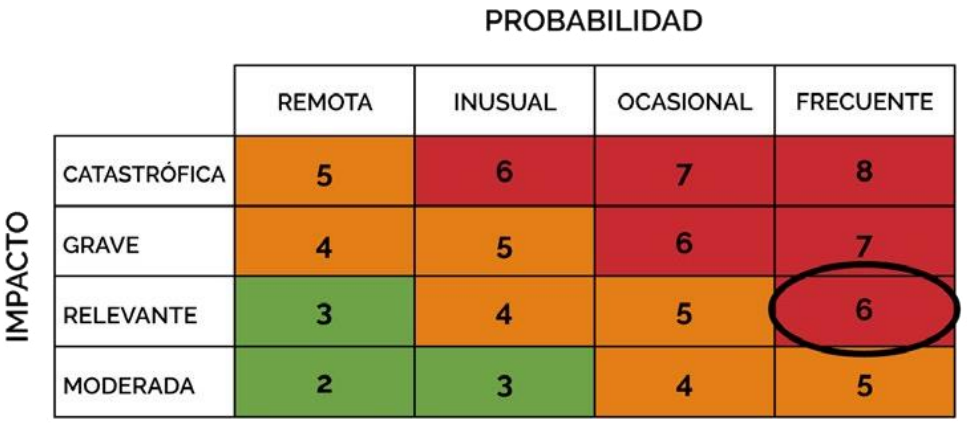
- El sistema de información impide la realización de compras (paralización o excesiva lentitud). En este caso nos encontramos con un cliente que compra frecuentemente y que desea cerrar la compra en ese momento. La suspensión del sistema provocaría que el cliente buscase el producto que desea comprar en otra web y si la experiencia es positiva, perder el cliente. Bajo esta perspectiva, considerando una ligera pérdida de clientes, el daño lo podemos clasificar como

relevante. La frecuencia la clasificaríamos como frecuente, al poder ocurrir varias veces al año.

- La plataforma logística se paraliza. Esto paralizaría la gestión de pedidos poniendo en peligro uno de los pilares del servicio al cliente, la entrega en poco tiempo. Y también paralizaría la gestión de comprar, pudiendo quedar desabastecido el almacén. El impacto podría dañar la imagen reputacional y provocar la pérdida de algunos clientes, por lo que el daño se clasifica como relevante.

- Canal de atención al cliente indisponible. No poder acceder a este canal en una empresa fundamentalmente virtual genera una alta insatisfacción entre los clientes, en especial si el objeto de la llamada es una reclamación. Esto puede generar un daño reputacional y una ligera pérdida de clientes, por lo que el daño se clasifica como relevante. Por poder presentarse esta situación más de una vez al año, por picos de llamadas, la frecuencia se determina como frecuente.

CLASIFICACIÓN DEL RIESGO.



RIESGO 1N.2 (Fallo en los sistemas TIC)

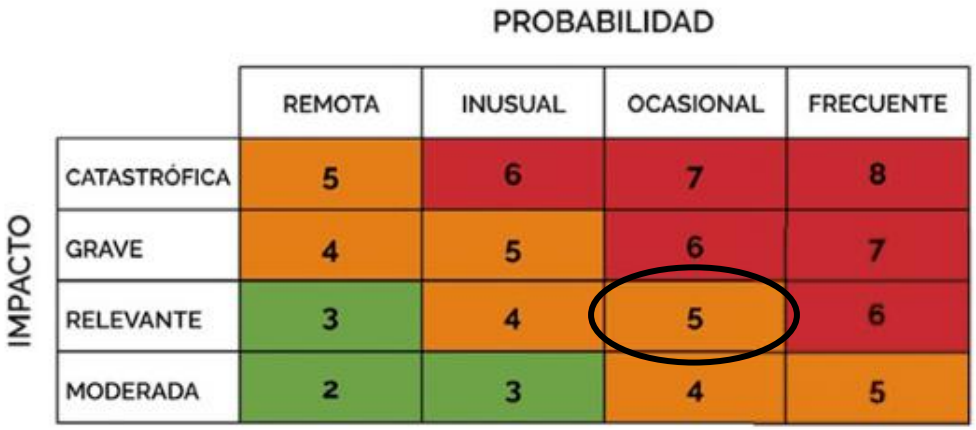
Aunque las causas de este riesgo son distintas a las del riesgo 1N.1, las consecuencias son similares.

Se añade una nueva causa para este riesgo:

- El sistema de información funciona incorrectamente. Errores en la gestión de operaciones con clientes o con los proveedores puede provocar la pérdida de los primeros y la correspondiente pérdida de reputación, compras no deseadas

a proveedores de mercancía no deseada, desabastecimiento de la mercancía deseada, etc. Se considera que es ocasional este tipo de incidente por esta causa y la intensidad relevante.

CLASIFICACIÓN DEL RIESGO.



RIESGO 1N.3 (Planificación inadecuada de DRP -Plan de Recuperación de Desastres- y Continuidad TIC).

Este tipo de riesgo podría provocar las siguientes situaciones no deseadas:

- Al ser una empresa grande y con una alta dependencia de las tecnologías, el 90% de sus ventas provienen de pedidos realizados por Internet, en caso de una inundación en el data center del tercero, esto haría que la actividad de la empresa basada en las ventas por Internet se viera gravemente afectada y en el período de tiempo necesario para restaurar los servicios, no se pudiesen suministrar ni recibir nuevos pedidos de los clientes ni recibir mercancía para surtir a los clientes.

- Si se produjese un incendio en su almacén de Málaga, esto pararía durante un tiempo la venta física que hacen en la tienda y al utilizar el edificio como almacén de los productos que se venden por Internet, aquellos productos que se tuviesen almacenados solo en este edificio no se podrían suministrar, al menos en los plazos de tiempo a los que están acostumbrados.

- Adicionalmente otras actividades también importantes, como es el servicio de atención al cliente.

CLASIFICACIÓN DEL RIESGO.

IMPACTO	PROBABILIDAD: REMOTA	INUSUAL	OCASIONAL	FRECUENTE
CATASTRÓFICA	5	6	7	8
GRAVE	4	5	6	7
RELEVANTE	3	4	5	5
MODERADA	2	3	4	5

RIESGO 2N.1 (Seguridad Física de la TIC inadecuada).

Al estar los sistemas de la empresa ubicados en un Data Center de un tercero a cientos de km. de la empresa, hace que la empresa sea más dependiente de un tercero y que la seguridad física esté correctamente diseñada para que nos dé las garantías necesarias.

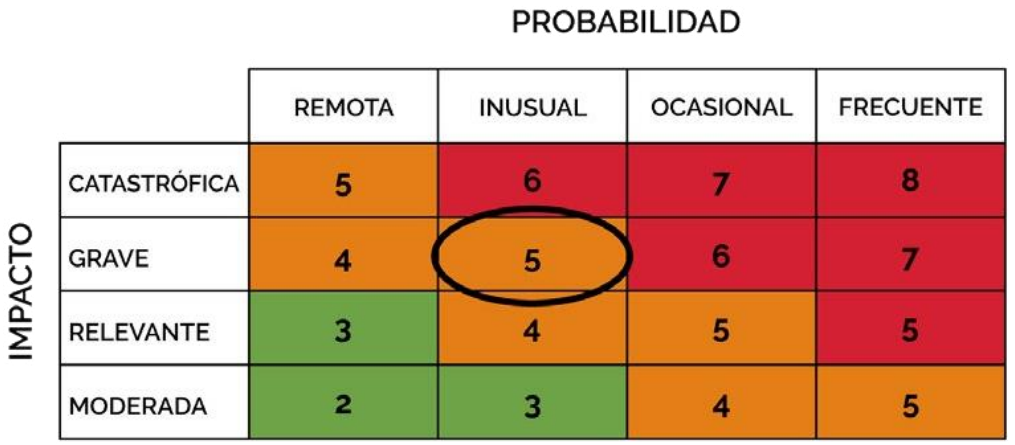
Este tipo de riesgo podría provocar las siguientes situaciones no deseadas:

- Que se robasen de la base de datos de clientes la información referente a sus datos de contacto, esto podría tener consecuencias como que no se pudiese contactar con estos clientes para enviarles ofertas y cualquier otra campaña de marketing. También que los datos de contacto de estos clientes fueran accesibles para terceras partes no autorizadas, revendidas, etc. Esto podría traer consecuencias derivadas de la aplicación de la nueva normativa de protección de datos y/o daños para la imagen reputacional de la empresa.

- El que un empleado deshonesto, o despedido a su juicio injustamente pudiese hacer una manipulación o copia de la información de la base de datos de los clientes, es una situación que también podría darse con las mismas consecuencias que en el caso anterior.

- En el caso de una catástrofe natural, que afectase a las instalaciones donde se encuentran físicamente los sistemas informáticos, podría causar la pérdida total o parcial de los sistemas y del centro de datos. Paralizándose casi totalmente la actividad de la empresa por la alta dependencia tecnológica que tiene la misma, tanto en la venta, como en los procesos internos y externos.

CLASIFICACIÓN DEL RIESGO.



RIESGO 3N.1 (Controles inadecuados sobre el cambio o el desarrollo TIC).

Un proceso de control de cambios que no logre establecer normas y procedimientos para las propuestas de cambio y satisfacer las necesidades de la organización puede poner en peligro la integridad de los datos y las necesidades del sistema o de los usuarios de negocio. Si los procedimientos adoptados para la implementación del cambio no son eficaces, se podrían dar los mismos riesgos que si no existen. No adoptar procedimientos sistemáticos o respetar los existentes para iniciar las solicitudes de cambio, pruebas, documentar cambios, y autorizar cambios en los sistemas y procesos antes de la implementación puede resultar en cambios no exitosos. Además, la incapacidad para rastrear donde se habían hecho cambios podría retrasar la corrección de cualquier problema o incluso agravarlo.

Este tipo de riesgo podría provocar las siguientes situaciones no deseadas:

- Los daños en los datos por errores en la gestión de los cambios pueden dar errores en procesos críticos: venta online, plataforma logística y canal de atención al cliente. La frecuencia en ambos casos sería inusual y el impacto podría considerarse grave, al tener una dependencia completa de los sistemas de información.

- Los daños por errores en la gestión de cambios en las comunicaciones (externas o internas) impedirían la prestación de casi la totalidad de los servicios: venta online, logística (control de stock, pedidos, salvo la entrega de producto a cliente por las entregas en curso), canal de atención al cliente (generando la correspondiente insatisfacción de no poder atender a tiempo), además de los procesos de marketing basados en canales online y Social Media. Podría considerarse el riesgo como inusual y de intensidad grave.

- Los daños en la gestión del cambio en las aplicaciones, al ser mayoritariamente desarrollos propios, generarían un impacto relevante, en función de la criticidad de dicho error, si pudiera ser subsanable en un espacio de tiempo razonable; si conllevara una reparación completa generaría fallos en precios, datos de terceros, pedidos, etc. Al haber adecuado los desarrollos de sus aplicaciones a la tipología de su producción se considera un riesgo inusual, aunque relevante en su impacto.

CLASIFICACIÓN DEL RIESGO.

IMPACTO \ PROBABILIDAD	REMOTA	INUSUAL	OCASIONAL	FRECUENTE
CATASTRÓFICA	5	6	7	8
GRAVE	4	5	6	7
RELEVANTE	3	4	5	5
MODERADA	2	3	4	5

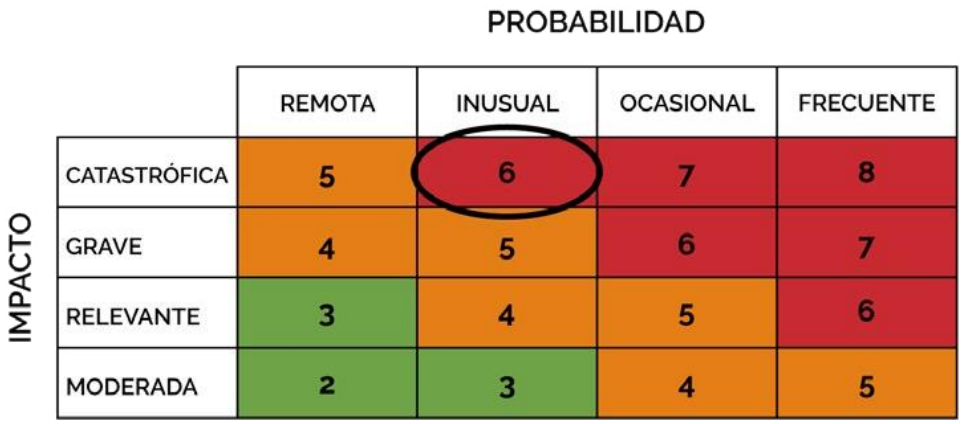
RIESGO 3N.2 (Arquitectura TIC inadecuada).

El diseño de la arquitectura que no incorpora o no permite incorporar entornos técnicos avanzados para el desarrollo o la mejora de aplicaciones en el futuro, puede llevar a obstaculizar las perspectivas futuras de crecimiento de la organización y exponerla a una falta de control del riesgo extrema.

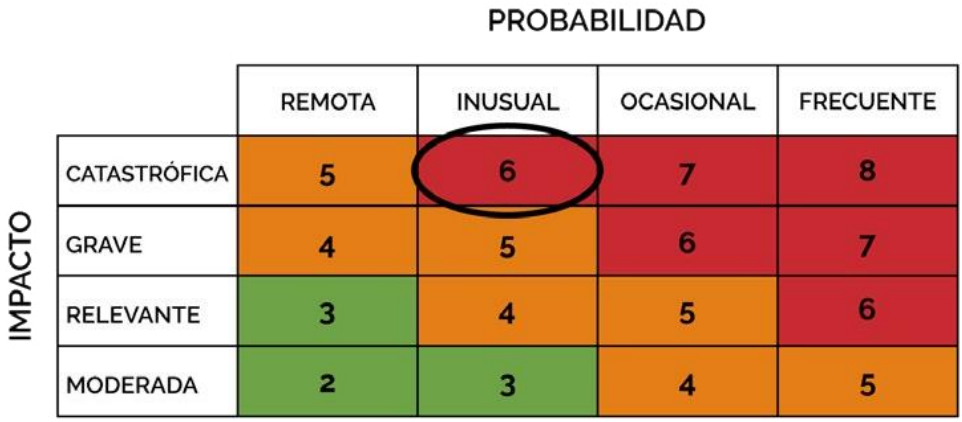
Un mal diseño de la arquitectura de TI, podría provocar casos de negocio no considerados, incluido el impacto en los usuarios, gestión de impuestos, y los requisitos reglamentarios multi-jurisdiccionales, así como mala imagen frente a nuestros clientes y pérdida de negocio.

Este tipo de riesgo podría provocar las siguientes situaciones no deseadas:

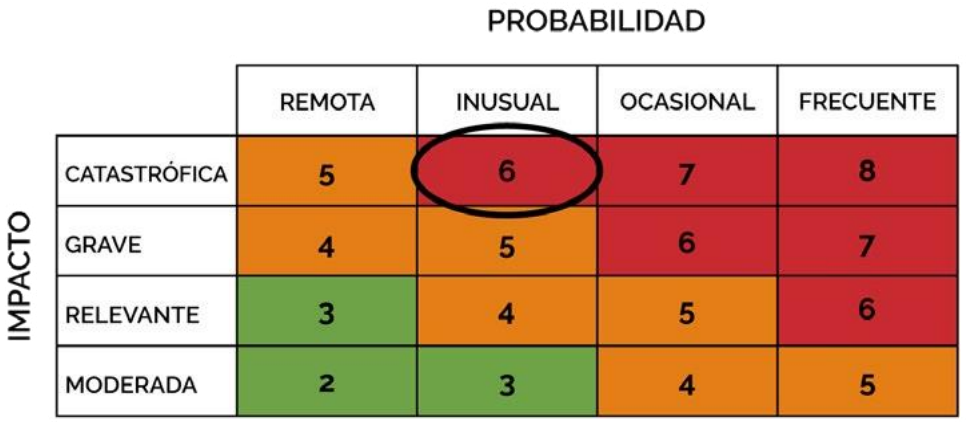
- La falta de adecuación a un negocio cambiante hace que se puedan perder clientes por falta de acceso a la oferta, lo que hace que para un negocio de este tipo es inviable no adecuar la actividad a una tecnología suficientemente adecuada, no pudiendo competir en el mercado.



- En caso de no utilizar la tecnología adecuada, la pérdida de capacidad de negocio para continuar existiendo tiene un impacto muy elevado, incluso el cierre del negocio.



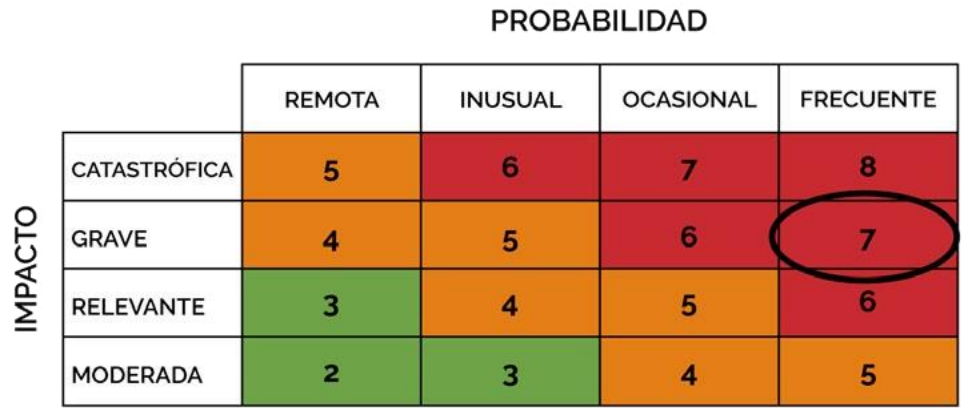
CLASIFICACIÓN DEL RIESGO.



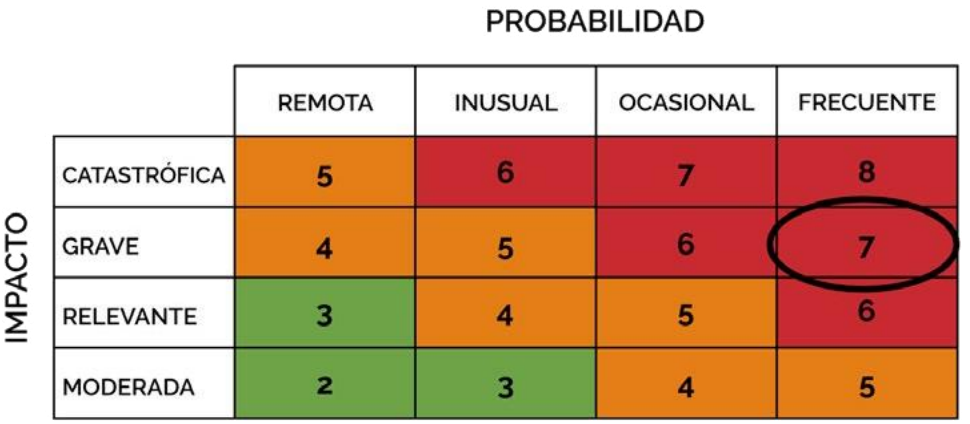
RIESGO 4N.1 (Procesado o manejo inadecuado de TIC).

Este tipo de riesgo podría provocar las siguientes situaciones no deseadas:

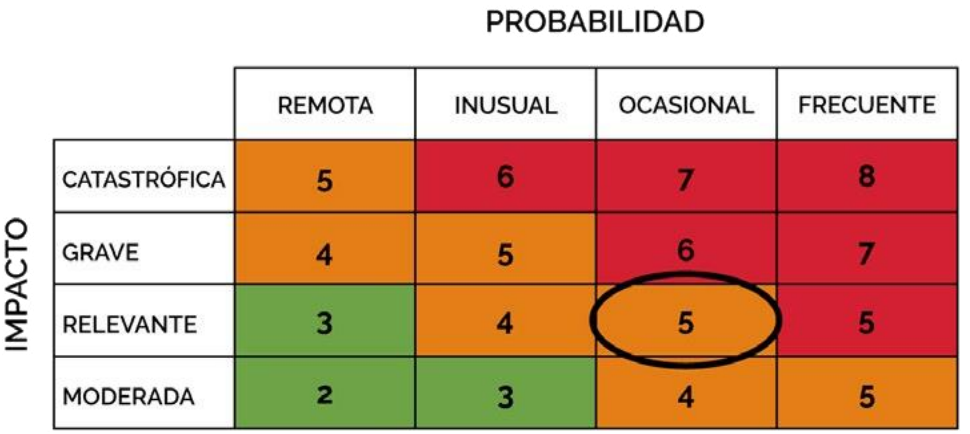
- Los errores o fallos en el sistema de información conllevarían posibles daños en los datos alojados en los servidores de la empresa donde se custodia la información de todos sus procesos críticos: venta online, plataforma logística y canal de atención al cliente. Dado que los sistemas están en un Data Center de un tercero, este riesgo estaría analizado en el Riesgo 5.1, pero también sería aplicable en las integraciones de las aplicaciones del tercero con Compotec. La frecuencia en ambos casos sería frecuente y el impacto podría considerarse grave, al tener una dependencia completa de los sistemas de información.



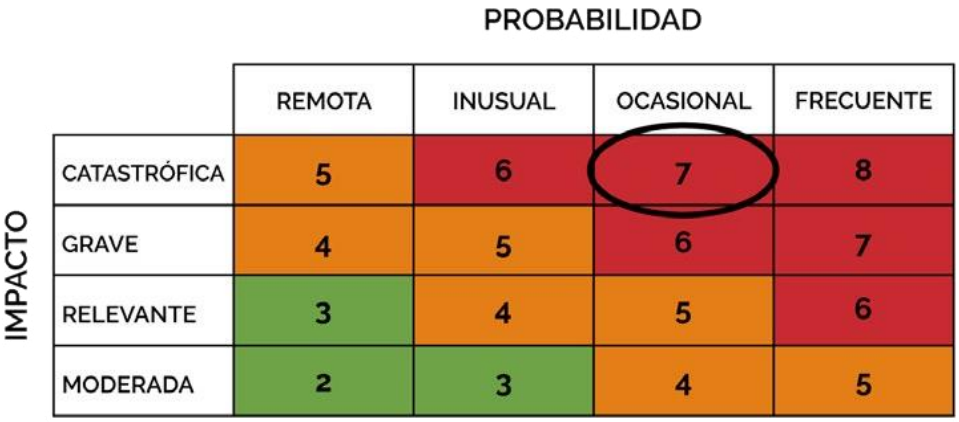
- Los errores o fallos en las comunicaciones (externas o internas) impedirían la prestación de casi la totalidad de los servicios: venta online, logística (control de stock, pedidos, salvo la entrega de producto a cliente por las entregas en curso), canal de atención al cliente (generando la correspondiente insatisfacción de no poder atender a tiempo), además de los procesos de marketing basados en canales online y Social Media. Podría considerarse el riesgo como frecuente y de intensidad grave.



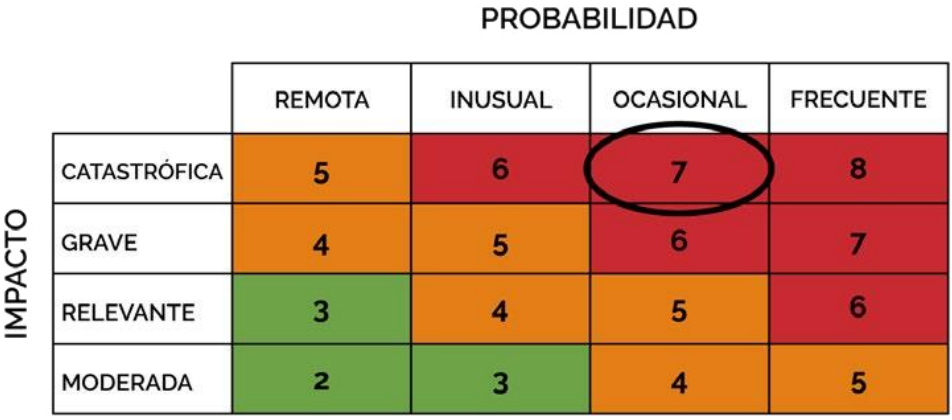
- Los errores o fallos en las aplicaciones, al ser mayoritariamente desarrollos propios, generarían un impacto relevante, en función de la criticidad de dicho error, si pudiera ser subsanable en un espacio de tiempo razonable; si conllevara una reparación completa generaría fallos en precios, datos de terceros, pedidos, etc. Al haber adecuado los desarrollos de sus aplicaciones a la tipología de su producción se considera un riesgo ocasional, aunque relevante en su impacto.



- Adicionalmente a cada análisis anterior, se incluirían las pérdidas de clientes y potenciales reclamaciones de estos, además de las sanciones regulatorias si hubiera alteraciones en los datos personales. Este impacto podría ser catastrófico por sus cuantías, especialmente por las sanciones de las AEPD, entre leves y graves (hasta el 2 % de la facturación: 6.000.000€), pero ocasional.



CLASIFICACIÓN DEL RIESGO.



RIESGO 4N.2 (Control inadecuado de los cambios a los datos en sistemas TIC en producción).

A diferencia del otro caso, el impacto sería mucho mayor, ya que el 100% de las ventas se hacen vía online y el impacto reputacional sería muy grave, pudiéndose migrar clientes a otros proveedores on line, si no se recupera el sistema en un breve espacio de tiempo. Sería obligatorio restaurar los sistemas urgentemente y llevar a cabo una gestión adecuada de los controles de modificación de los sistemas TIC.

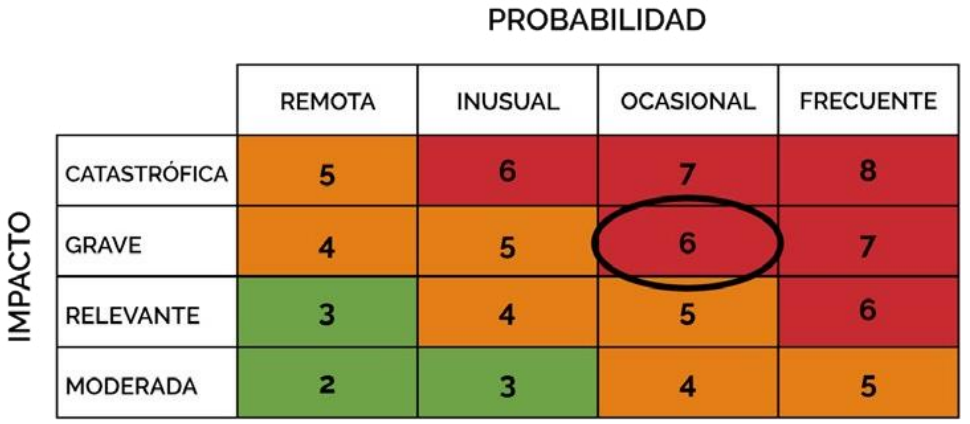
CLASIFICACIÓN DEL RIESGO.

IMPACTO \ PROBABILIDAD	REMOTA	INUSUAL	OCASIONAL	FRECUENTE
CATASTRÓFICA	5	6	7	8
GRAVE	4	5	6	7
RELEVANTE	3	4	5	5
MODERADA	2	3	4	5

RIESGO 5N.1 (Resilencia inadecuada de terceras partes).

En este caso, el impacto en ventas sería total sobre el volumen de la compañía durante el periodo de restauración y viendo que el proveedor tiene una resiliencia inadecuada, el tiempo podría ser demasiado alto como para no afectar al futuro de la compañía por la imagen ante el cliente y la alta competitividad que hay en el mercado. En cuanto a la pérdida de datos confidenciales de clientes y proveedores, el problema sería similar. En ambos casos, habría que tener en cuenta las responsabilidades que se pudieran derivar por contrato al proveedor, ya que el responsable directo ante posibles reclamaciones de terceros es la empresa de venta on line. Sería totalmente necesario cambiar de proveedor de la gestión de los sistemas TIC para la supervivencia de la empresa.

CLASIFICACIÓN DEL RIESGO.

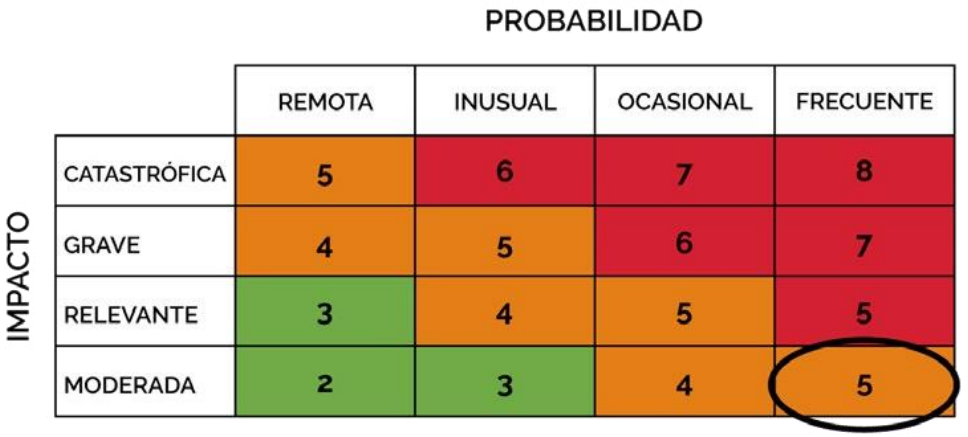


RIESGO 5N.2 (Gobierno inadecuado de la externalización).

De forma similar al Caso I, la inexistencia o ineficacia de un Gobierno Corporativo de Ciberseguridad determinará la ausencia o inadecuada gestión de los servicios IT externalizados e impedirá disponer de los planes de mitigación de riesgos cibernéticos que incluyan las adecuadas inversiones en soluciones de ciberseguridad y seguros.

En este caso, la degradación o fallos importantes del servicio debido a procesos ineficientes de preparación o control del proveedor de servicios subcontratado puede generar cualquiera de los riesgos de las anteriores naturalezas, en función del tipo de servicio que preste el proveedor. En logística, la falta de suministro y/o de entrega a cliente; en el Data Center, la inoperatividad de los sistemas de información. Por tanto, este riesgo será valorado en intensidad como la mayor de las que pueda identificarse en las anteriores si bien la frecuencia la consideramos moderada, al tener bien dimensionados los acuerdos con sus proveedores.

CLASIFICACIÓN DEL RIESGO.



5.3.2.- RIESGOS DE SEGURIDAD.

RIESGO 1S.1 (Ciberataques disruptivos o destructivos).

Las empresas del sector retail con un fuerte peso en el ámbito digital son especialmente sensibles a los ataques de tipo disruptivo debido a que:

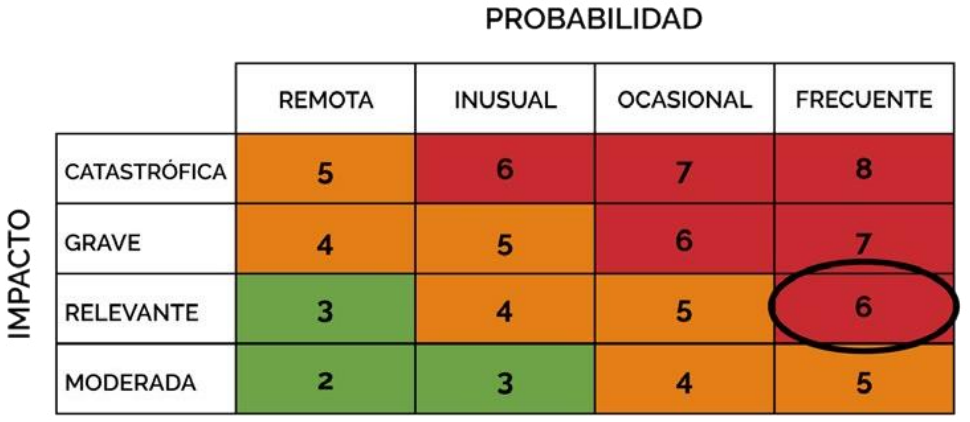
- Los problemas de sus páginas web tienen una fuerte repercusión en RRSS.
- El impacto en el nivel de satisfacción puede ser considerable pudiendo provocar un descenso repentino de los indicadores NPS de los clientes, que requieren un periodo de tiempo también considerable para su recuperación.
- El tipo de cliente en el sector retail digital tiene una baja tasa de reintento, en caso de no poder completar una compra, o bien es posible que se pierda la oportunidad de compra, o bien el potencial cliente busca el mismo producto por un precio similar en otra plataforma digital.

Aunque existen distintos tipos de ataques que pueden tener efectos disruptivos, los más comunes son los ataques de denegación de servicios, denominados DOS (por sus siglas en inglés Denial of Service) cuya técnica de ataque más común es el de la saturación de Internet de la organización, ya que supone el principal canal de acceso a los productos que ofrece la organización.

Las empresas que tienen una dependencia intensiva del canal Internet frecuentemente, son objetivo de grupos de cibercriminales que suelen solicitar el pago de una cantidad de dinero a cambio de no saturar dicho canal Internet. El modus operandi es variado, pero lo más habitual es que este tipo de grupos de cibercriminales suela tener "secuestrados" bajo su control miles de equipos de usuario a nivel global que pueden controlar a su antojo, pudiendo dirigir miles de solicitudes de acceso simultáneos y continuados al canal Internet de la compañía objetivo. Suelen realizar una pequeña prueba de concepto con la compañía objetivo de corta duración, pero suficiente para que la compañía objetivo perciba el volumen del ataque, posteriormente se ponen en contacto vía email explicando lo ocurrido y solicitando el pago de una cantidad monetaria bajo la amenaza de repetir con mayor intensidad y duración el ataque.

El impacto puede ser considerador como catastrófico dado que simplemente los costes directos de la facturación diarios son de cerca de 1 millón de € y su duración puede alargarse tanto como el grupo cibercriminal crea oportuno, por lo que es relativamente sencillo que se puedan superar los 2 millones de € de facturación, mientras que los costes operativos se mantendrían, así como los del coste del stock. Por lo que se considera que el presente riesgo debe estar en la parte más significativa de la matriz, todo ello sin entrar a valorar el impacto que podría tener en la satisfacción del cliente y en la tasa de repetición de compras de los clientes, aspectos que se consideran críticos para el funcionamiento de la empresa.

CLASIFICACIÓN DEL RIESGO.



RIESGO 2S.1 (Ciberataques y otros ataques externos basados en TIC).

La empresa de venta de dispositivos electrónicos “Componentes de Tecnología S.A.” (Compotec S.A.) presenta un elevado grado de dependencia de las nuevas tecnologías ya que su actividad económica se soporta en su mayoría en la venta online de sus productos a través de Internet. Si bien esta estrategia le permite una importante presencia geográfica sin necesidad de contar con infraestructura física, esta característica hace que la compañía quede especialmente expuesta a los riesgos y amenazas procedentes del ciberespacio, siendo los más destacables los siguientes:

- **Ataques ejecutados desde Internet o redes externas.**
  Este tipo de ataques se realiza con diferentes propósitos y utilizando una amplia variedad de técnicas. El principal objetivo es el control interno de los sistemas TIC, pudiendo ser diferentes las motivaciones (robo de información, chantaje, espionaje industrial, etc.).

  Entre las motivaciones, hay que considerar que se trata una empresa de cierto éxito con una página web de ventas online muy visitada. Por ello, no es descartable que pudiera ser atacada para modificarla con fines propagandísticos (hacktivismo) o bien con intención de comprometerla para “infectar” con malware a los potenciales visitantes, e incluso para utilizarla como punto de entrada para hacerse con el control de los sistemas TIC de la compañía. Tratándose la página web de un desarrollo propio por personal no especializado, se hace más probable un escenario de este tipo. La detección de fallos de seguridad en páginas web publicadas en Internet es habitual ya que se realizan escaneos (búsquedas) de forma automatizada por parte de los ciberdelincuentes, por lo que no es improbable que un fallo de este tipo sea detectado y aprovechado por actores malintencionados.

  Otra motivación, habida cuenta que la empresa se encuentra inmersa en un proceso de revalorización previo a su venta, podría ser tratar de afectar negativamente a la reputación de la compañía, por ejemplo, mediante la exfiltración de información de los clientes, de forma que perdiera parte de su valor. Detrás de una acción de este tipo podría estar un comprador con pocos escrúpulos. Este escenario pone de manifiesto que la valoración de un riesgo puede variar en función del contexto de cada organización. No obstante, no es este tipo de acciones no es habitual en España, si bien cada vez se dan a conocer más casos de actores malintencionados que aprovechan las nuevas tecnologías con intención de dañar la reputación o recursos de un adversario, en cualquier ámbito (política, comercio, etc.).

Sin embargo, el móvil más habitual y probable sería el económico; en concreto, un actor malicioso podría distribuir un malware que cifrase los archivos de información (ransomware) pidiendo un rescate a cambio de su recuperación. Una acción de este tipo puede tener un efecto notablemente negativo para la actividad de la organización si no existen planes de copia de seguridad y recuperación adecuados. Otra técnica de extorsión, también relativamente habitual, es la de amenazar con hacer pública información robada a la compañía en caso de no recibir un pago, con el riesgo para la reputación de la compañía que ello supondría. Uno de los principales vectores para este tipo de ataques es la utilización de técnicas de ingeniería social a través del correo electrónico, medio de comunicación habitual de la actividad interna y externa (Canal de Atención al Cliente) de la organización objeto de estudio.

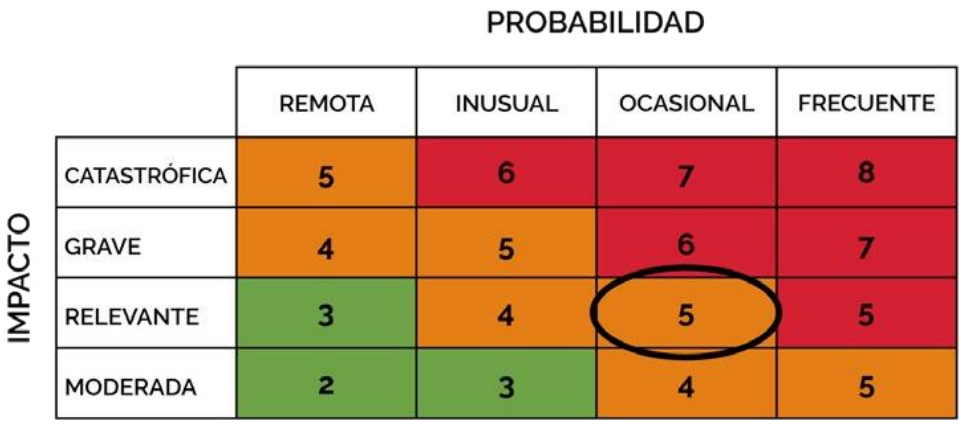
El impacto de un ataque por ransomware es similar a un ataque disruptivo de DOS desde el punto de vista operativo, ya que el principal aspecto al que afecta es a la cadena de suministro de los servicios de la página web que se ofertan al cliente. No obstante, a este coste habría que añadirle los costes operativos de:

1. Recuperación de los sistemas a un estado válido anterior y libre de software malicioso.
2. Análisis forense de las causas que han posibilitado el ataque.
3. Resolución de las deficiencias de seguridad que expongan a la organización a este tipo de situaciones de alto riesgo.

Cabe señalar que en muchas ocasiones la realización de este tipo de trabajos suele llevar más de un día, pero también es importante señalar que la empresa Compotec es una empresa relativamente joven que ha creado sus sistemas de información a medida y dispone de infraestructura en cloud por lo que se le asume cierta agilidad a la hora de poder realizar una marcha atrás de sus sistemas de información.

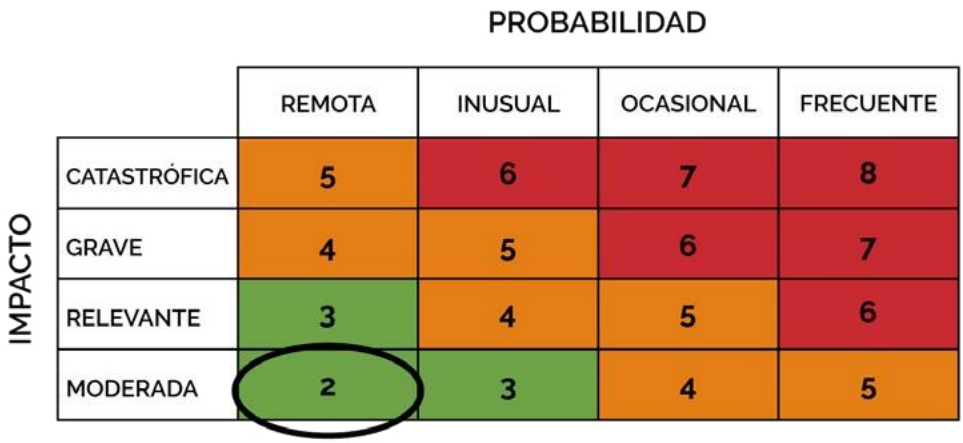
A este coste es cierto que habría que sumarle el coste reputacional, legal y de responsabilidad civil contra terceros, pero dado que el coste reputacional es el más relevante y que existen precedentes que demuestran que si la empresa se comporta de forma diligente, transparente y continúa ofreciendo un buen servicio a sus clientes, dicho coste queda en gran parte amortiguado por la solvencia reputacional y el valor que ofrece a sus clientes.

A la vista de lo anteriormente expuesto y como resumen, estimamos que la posibilidad de que ocurra es OCASIONAL y los efectos pueden ser RELEVANTE.



- **Ejecución de transacciones fraudulentas de pago (e-banking).**
  Compotec S.A. utiliza pasarelas de pago de terceros en su canal de ventas online. Por su propia concepción y diseño, este tipo de pasarelas cuentan con medidas adecuadas de seguridad ya que son desplegadas y gestionadas por las compañías financieras, quienes alertarían a la compañía de cualquier movimiento inusual, por lo que podría detectarse y corregirse en un breve plazo de tiempo.

  Por ello, estimamos que la posibilidad de este riesgo es REMOTA y la intensidad MODERADA.



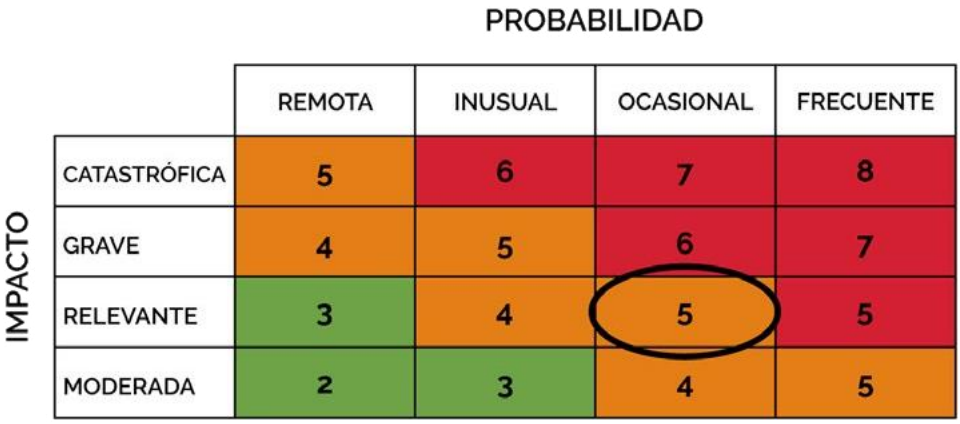
- **Ataques a las comunicaciones y conversaciones.**
  El objetivo de este tipo de acciones es interferir en las comunicaciones de la organización para obtener información, de forma no autorizada, que pueda ser utilizada para cometer fraudes. Analizaremos diferentes escenarios.

  Un escenario potencial sería la interceptación de las comunicaciones de un cliente al acceder a la web de compras online. Hoy día cualquier canal de compras online está cifrado (por supuesto, cualquier pasarela de pago) por lo que lo más probable sería que los ciberatacantes hubieran comprometido directamente el equipo remoto del cliente. En este caso, cualquier actuación fraudulenta (por ejemplo, realizar una compra en nombre del ten cliente) tendría un alcance muy limitado y además estaría fuera de la esfera de responsabilidad de la compañía.

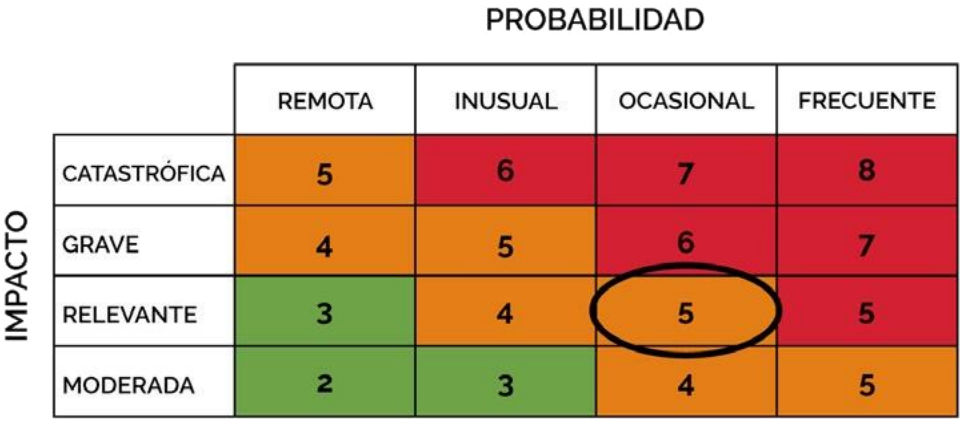
  Un segundo escenario sería que un actor malintencionado comprometiera uno o varios equipos de la compañía y pudiera acceder a las comunicaciones internas. Esta situación podría tener un impacto negativo elevado, pero requiere de un alto grado de sofisticación por parte de los atacantes, siendo en consecuencia un escenario muy improbable.

  Un tercer escenario sería la utilización del correo electrónico para conseguir algún objetivo malintencionado. Como ya se puso de manifiesto anteriormente, la actividad de Compotec S.A., en particular el Canal de Atención al Cliente y a ciencia cierta, de gran parte de su actividad (comunicaciones con proveedores, comunicaciones internas, etc.), se soporta en el uso del correo electrónico, por lo que la compañía resulta particularmente expuesta a riesgos derivados del uso de este medio. Un caso particular son los conocidos como ataques BEC (Business Email Compromise) o “fraude del CEO”. Se trata de un tipo de estafa que presenta diferentes variantes en su “modus operandi”, pero con la característica común de que los ciberdelincuentes aprovechan este medio, el correo electrónico, para suplantar ilegítimamente a un tercero y engañar a la víctima. Un caso habitual es que los ciberdelincuentes suplanten a un directivo para solicitar a un empleado (la víctima) que realice un pago para un “operación confidencial” en una determinada cuenta, que por supuesto está en manos de los ciberdelincuentes. También otro caso habitual es que los ciberdelincuentes se hagan pasar por un proveedor de la empresa “víctima” que “solicita que se cambie el número de cuenta en la cual se abonan sus servicios”. Como en el caso ejemplo anterior, el nuevo número de cuenta estará en manos de los ciberdelincuentes.

Como resumen de los escenarios anteriores, estimamos que este riesgo tiene una frecuencia OCASIONAL y una intensidad RELEVANTE.



CLASIFICACIÓN DEL RIESGO.



RIESGO 2S.2 (Seguridad TIC interna inadecuada).

Los daños que pueden derivarse si se materializa la amenaza están relacionados con la pérdida de confidencialidad, integridad y disponibilidad de la información y el impacto reputacional y/o económico para la empresa Componentes de Tecnología S.A. si trascienden las consecuencias.

Pormenorizando en cada uno de los riesgos particulares de este tipo de riesgos, podríamos enfrentarnos a las siguientes situaciones:

- **Obtención de acceso no autorizado a sistemas TIC de la empresa Componentes de Tecnología S.A. para diferentes propósitos** (por ejemplo, fraude, realizar y ocultar actividades comerciales ilegales, robo de datos, activismo/sabotaje). Puede materializarse cuando se produce una sustracción/usurpación de credenciales, o se obtienen accesos y/o privilegios para los que no se está autorizado.

  Esta amenaza se relaciona con los controles de acceso lógico a sistemas y aplicaciones, en el escenario descrito no relata nada acerca de los controles implantados se presupone dado el volumen de negocio que cuenta con un sistema de seguridad lógica adecuado para impedir este tipo de accesos, así como un nivel de parcheado de sistemas y frecuencia de actualización de software aceptable, así como un plan de continuidad del negocio con procedimientos de recuperación ante desastres vigentes y probados con el proveedor del Data Center donde están alojados los servidores.

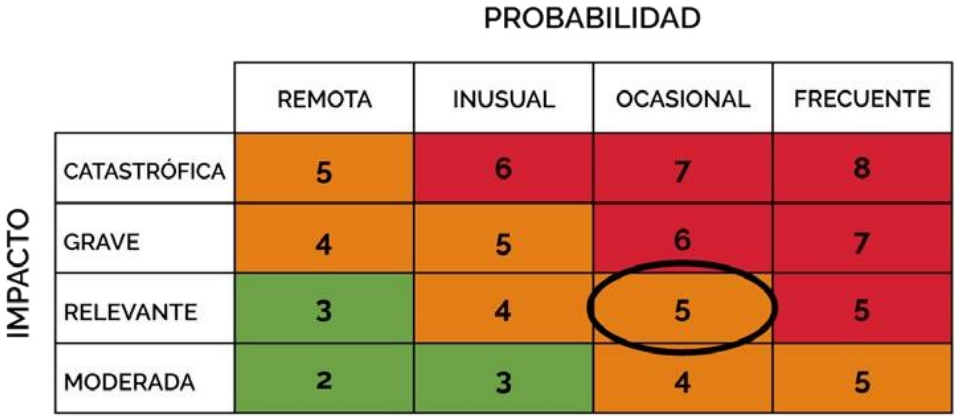
  A pesar de que la frecuencia pueda variar, existirían varios escenarios posibles en caso de materializarse el acceso no autorizado, dependiendo tanto del tipo de acceso conseguido (usuario de servicio de mantenimiento de sistemas, usuarios de gestión de cada uno de las aplicaciones informáticas de la empresa, etc.) como del impacto, que podría ser grave debido a la virulencia de las acciones que podrían realizar los atacantes, dada la gran variedad de técnicas que podrían realizar, como robo de credenciales con el máximo privilegio en el sistema informático de la empresa, que podrían explotar vulnerabilidades del sistema o desplegar software malicioso provocando la interrupción total del servicio, afectando a la casi totalidad de los procesos críticos del negocio.

  Como resumen de los escenarios anteriores, estimamos que este riesgo tiene una frecuencia OCASIONAL y una intensidad RELEVANTE.

- **Caso de no disponibilidad del servicio.**
  La falta de disponibilidad de los sistemas críticos (venta online, plataformas de logísticas y canal de venta online) y atendiendo al volumen de facturación anual, repartido por días sería (300M /365 días) sale una facturación diaria de 821.917,81 euros/día. Si tenemos en cuenta que la principal virtud de la empresa es el periodo de entrega en 24 horas territorio nacional, suponemos que, en caso de indisponibilidad del servicio, como mínimo tendríamos el doble, 48 horas para que los planes de DRP activaran de nuevo el sistema, por lo que las pérdidas en dos días ascenderían a 1.623.835,62 euros, clasificado de relevante, suponiendo la

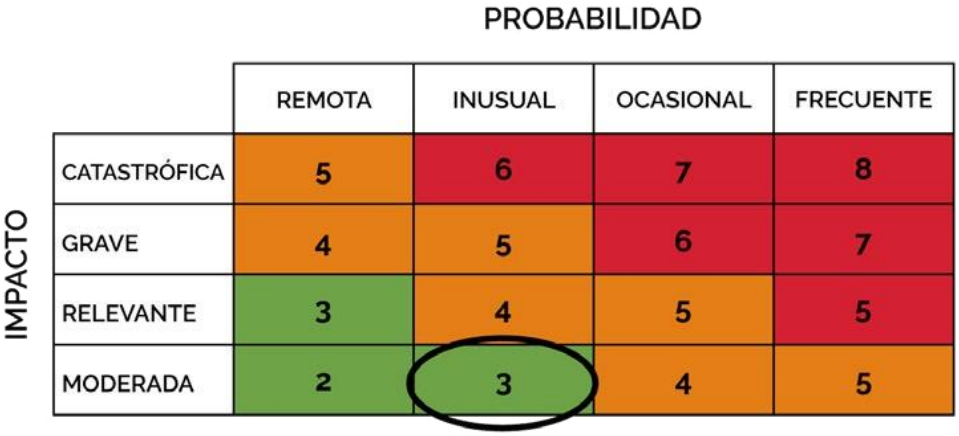
frecuencia como ocasional debido al grado de madurez de Ciberseguridad que se presupone tiene la compañía.

Entendemos que esas 24 horas de indisponibilidad no supondría excesiva pérdida de fidelización de clientes.



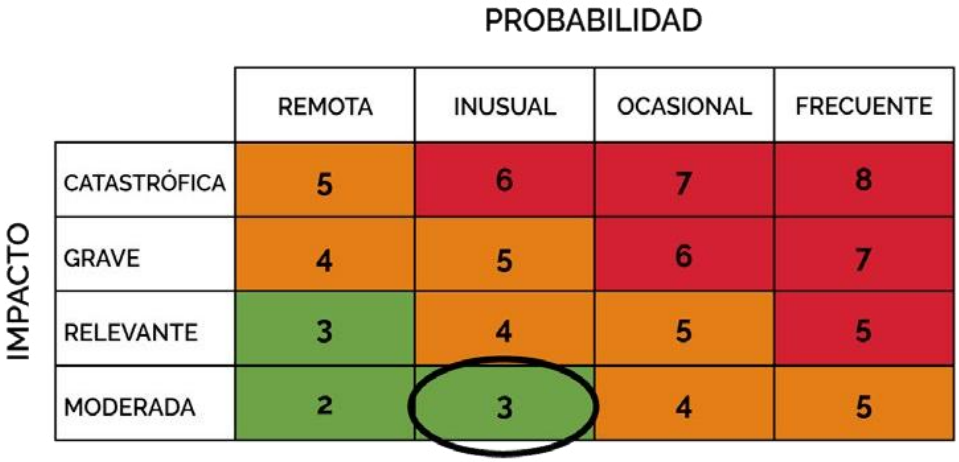
- **Caso de fuga de información.**
  Este supuesto, lo analizaremos bajo el supuesto de ofrecer sistema de pago on-line con TPV virtual con pasarelas de pago en la que no se almacena ningún dato de tarjeta de crédito en los sistemas de la empresa, lo que hace el riesgo de pérdida de datos de tarjeta de crédito despreciable.

  De no ser así el coste de los registros podría ser mucho mayor y la fuga de información podría centralizarse en información de clientes (datos de tarjeta y datos personales), proveedores, secretos profesionales en cuando a distribución y precios de componentes, etc. Atendiendo al coste medio estipulado por pérdida de registro en una compañía de 225 euros (según rango establecido por el instituto Ponemon) y considerando el millón de clientes que tiene la empresa, las pérdidas ascenderían a 225.000.000 de €, resultando ser catastrófica, independientemente de la frecuencia con que se pudiese dar este escenario. Para completar el estudio con todas las variantes, estimamos que la frecuencia sería inusual.



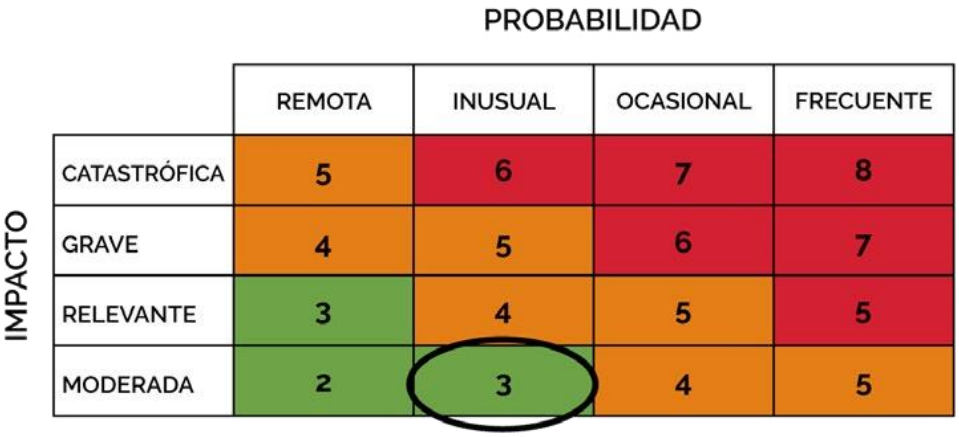
- **Manipulaciones no autorizadas de las TIC** debido a procedimientos y prácticas inadecuados de gestión de acceso a las TIC.

  Existe un grado de automatización en todos los procesos de manera que existe poco margen de manipulación de usuarios en el sistema integral de gestión de la compañía, por tanto este riesgo no se considera importante, con frecuencia INUSUAL e intensidad RELEVANTE si atendemos a la pérdida estimada de un día por posibles deficiencias en los sistemas.



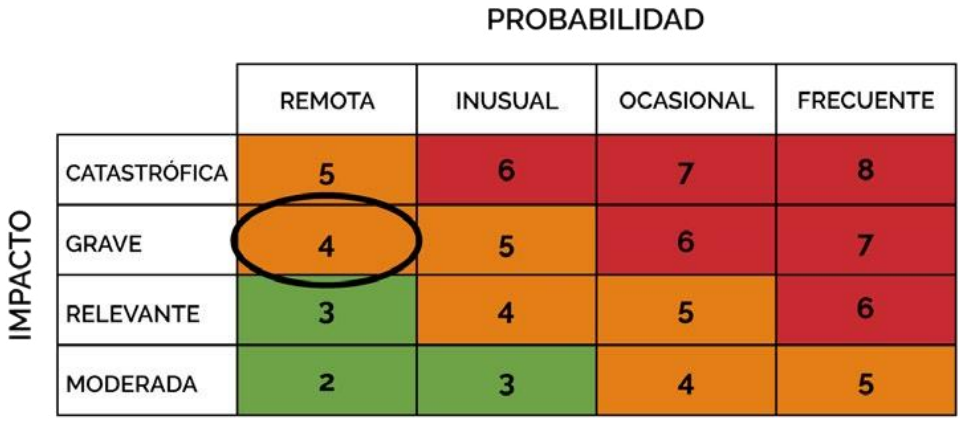
- **Amenazas de seguridad debido a la falta de conciencia de seguridad** por la cual los empleados no entienden, descuidan o no cumplen con las políticas y procedimientos de seguridad de las TIC.

  Es poco probable debido a la poca interacción sobre procesos críticos de los usuarios normales del sistema. Aunque es un riesgo que se puede materializar dado el que en muchas ocasiones los siniestros de seguridad suelen tener como raíz la falta o error de una persona de la organización, el riesgo en si no es el causante del daño sino que suele emplearse como un elemento o puerta de entrada para que los cibercriminales realicen algún otro ataque como el caso de fuga de información o ataques disruptivos mediante ransomware. Pero en dichos casos ya se encuentran incluidos dichos supuestos.



- **El almacenamiento no autorizado o la transferencia de información confidencial** fuera de la institución.
  Casuística similar a la de fuga de información, cuyo impacto y consecuencias ya están incluidas en dicho epígrafe. No obstante la gran diferencia en este caso se basa en que los escenarios que pudieran llevar a la empresa a tener unas consecuencias tan relevantes estarían bajo el marco de control de la empresa dado que estamos hablando de transferencias conocidas y autorizadas por la compañía que deberán hacerse bajo un marco de control técnico y legal adecuado. A pesar de que las multas pudieran llegar a los 20 millones de € o el 4% de la facturación, no sería el caso dado que la empresa no almacena datos especialmente protegidos (según define la GDPR) aspecto que limitaría una hipotética sanción aunque si maneja datos financieros y económicos de sus clientes, por lo que es razonable

pensar que un escenario de pérdida máxima (en la que concurriera negligencia y ausencia de debida diligencia) la sanción pudiera llegar a los 2 millones de €.



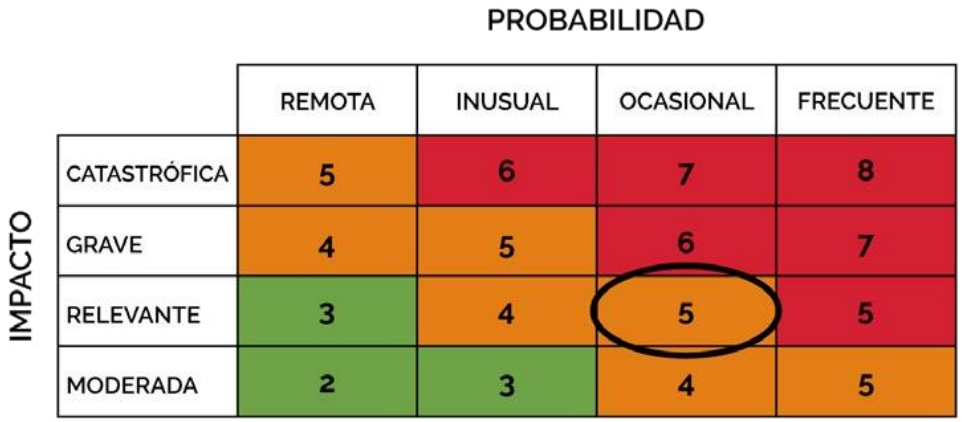
RIESGO 3S.1 (Gestión inadecuada del ciclo de vida y parcheado).

Al igual que en el caso del hotel, el presente riesgo está muy relacionado con el riesgo 2S.2 (seguridad inadecuada de TIC) ya que el principal riesgo que plantean los sistemas desactualizados es su vulnerabilidad frente a ataques ya conocidos, para los que en muchos casos suelen existir programas informáticos que posibilitan de forma sencilla a un potencial atacante el materializar estos ataques.

Al igual que en el caso del hotel, la motivación del atacante es la que va a ayudar a modelar el riesgo. En el caso de una empresa de retail de ámbito digital uno de los principales activos que suele tener es el de los datos de pago del cliente, por lo que el caso de fuga de información debe tenerse en cuenta, en aquellos casos que existan datos de tarjetas de crédito de los clientes.

Para el cálculo de la probabilidad/frecuencia se puede tener en cuenta que lo más habitual es que todos los meses los fabricantes de SW publiquen sus boletines de seguridad en los que se incluyen los parches a instalar. Aunque no está especificado en el caso lo más habitual es que en empresas maduras los ciclos de mantenimiento de SW estén comprendidos entre 1 y 6 meses, por lo que asumiendo una ventana de mantenimiento de 3 meses (sin tener en cuenta posibles incompatibilidades del software que utilice que suele ser el principal impedimento para la actualización de los sistemas por dependencias entre estos), implicaría que durante este tiempo los sistemas serán vulnerables.

CLASIFICACIÓN DEL RIESGO.



El color rojo mostraría el riesgo al que se encuentra expuesto durante el periodo de tiempo de los 3 meses que los sistemas de este se encuentran desactualizados, y el naranja se correspondería con la ventana de tiempo en el que se actualizara.

No obstante, también existe la posibilidad de otro tipo de fraude que puede servir de motivación para potenciales atacantes ya que la empresa maneja productos tecnológicos de alta demanda y precio elevado que pueden ser objeto de fraude. Aunque cualquier vulneración de los sistemas para la generación fraudulenta de pedidos falsos siempre tendría un impacto muy inferior (p.e.: cien teléfonos de alta gama de un valor de 1.000€) y la empresa podría disponer de un mayor margen de reacción para la detección y toma de medidas pertinentes.

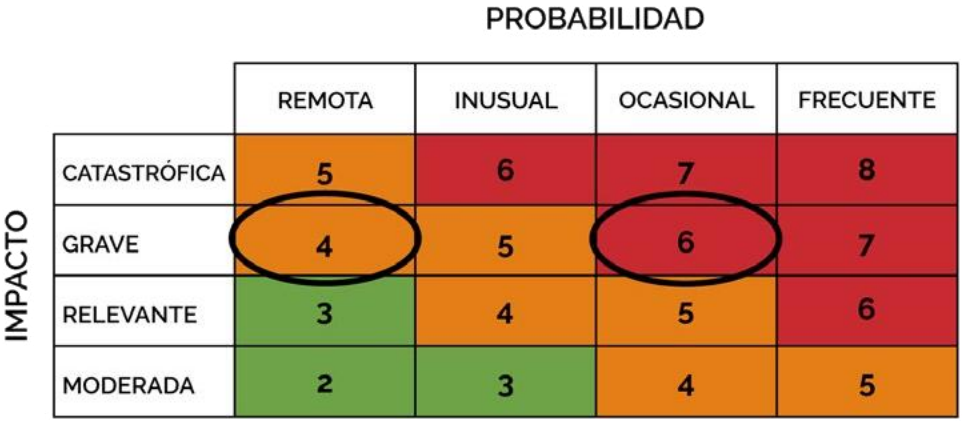
RIESGO 4S.1 (Diseño inadecuado de los controles de validación de datos en sistemas TIC).

Este riesgo se refiere a los efectos negativos que podrían producirse sobre la actividad de la compañía si los datos que se almacenan y procesan mediante los sistemas informáticos fueran incompletos, inexactos, inconsistentes o incoherentes debido a un proceso de validación incorrecto o inexistente en los flujos de información entre los distintos sistemas.

Compotec S.A. es una organización con un elevado grado de digitalización. Su actividad se soporta en diferentes sistemas informáticos que deben intercambiar información de forma permanente, segura y eficiente para asegurar los plazos de suministro a los clientes, principio clave sobre el que se sustenta el éxito de la compañía.

Algunos de los procesos críticos de la compañía (venta online, gestión de stock y de pedidos) se gestionan mediante plataformas tecnológicas que han sido desarrolladas internamente por la propia compañía. Este hecho, dado que se trata de personal sin cualificación específica, puede conllevar que algunos controles y tratamientos de los datos no se hubieran realizado de forma adecuada, poniendo en riesgo la actividad de la organización si se produjera cualquier fallo que afectase a la disponibilidad de los sistemas o, aún peor por la dificultad para detectarlo, a la integridad de los datos. Sin embargo, habitualmente una situación de este tipo se descubriría en las fases tempranas de funcionamiento de las propias aplicaciones y, aunque su resolución hubiera supuesto costes adicionales y afecciones a la operación, el uso prolongado en el tiempo de los sistemas informáticos habría permitido detectar y corregir al menos los fallos más habituales, si bien no es descartable que se dieran otros nuevos de vez en cuando (estimamos que en alguna que otra ocasión, cada 10 años). Por otra parte, dada la dependencia tecnológica de esta compañía, un fallo de este tipo podría provocar alguna pérdida de ventas o un incumplimiento en el suministro de materiales, con cierta afección negativa sobre la percepción de los clientes, o bien causar algún problema en la gestión de proveedores, no siendo desdeñable ninguna de estas situaciones.

CLASIFICACIÓN DEL RIESGO.



RIESGO 5S.1 (Seguridad inadecuada de terceras partes).

La empresa Componentes de Tecnología S.A tiene varias terceras partes que infieren de manera directa sus sistemas TIC:

- Empresa mantenedora del Data Center.
- Entidad bancaria de pasarela de pagos.
- Conexión con plataformas de marketing.
- ISP de telecomunicaciones.

Para todas estas empresas y los riesgos asociados a fallos son debidos a una inadecuada seguridad estarían en parte relacionados con los distintos acuerdos establecidos con los mismos, y a la existencia de cláusulas especiales de transferencia de riesgos, como podrían ser seguros de ciberriesgos.

De manera general, habría que distinguir, además, en el tipo amenaza materializada en el tercero y el efecto directo en la empresa.

Se pueden distinguir varias casuísticas, en relación al grado de dependencia en los sistemas de información de las terceras partes y la empresa.

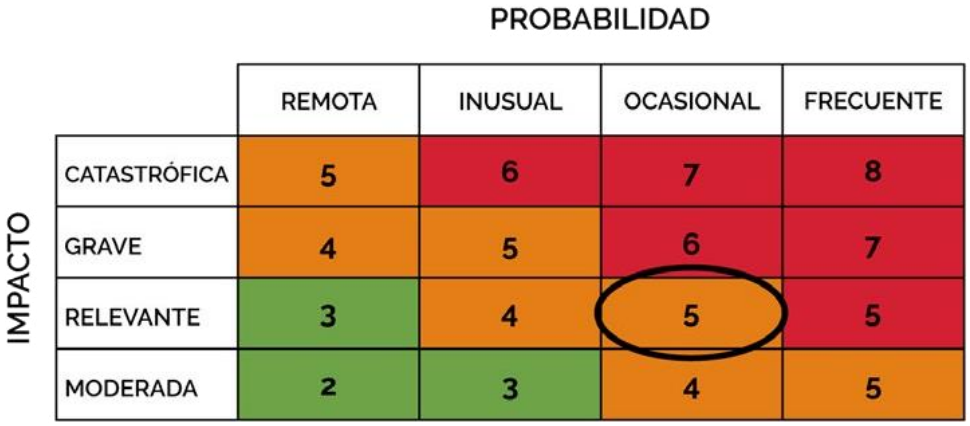
El riesgo más común y directamente relacionado sería la falta de disponibilidad de los servicios debido a problemas en el proveedor del Data Center, pérdida de conectividad con plataformas y entidades bancarias y habría que tenerse en cuenta los distintos acuerdos de servicio o (SLA´s) establecidas.

Profundizando en las causas, de todos los posibles efectos, el más grave sería la falta de disponibilidad de los servicios y la valoración sería la misma que en el caso **RIESGO 2S.2: Seguridad TIC interna inadecuada**, Caso de no disponibilidad del servicio.

IMPACTO \ PROBABILIDAD	REMOTA	INUSUAL	OCASIONAL	FRECUENTE
CATASTRÓFICA	5	6	7	8
GRAVE	4	5	6	7
RELEVANTE	3	4	5	5
MODERADA	2	3	4	5

5.4- MAPA DE RIESGOS.

A continuación, se representan todos los riesgos analizados en el mapa de riesgos.



LEYENDA:

- RIESGO 1N.1 (Gestión inadecuada de la capacidad).
- RIESGO 1N.2 (Fallos de los sistemas TIC).
- RIESGO 1N.3 (Planificación inadecuada de DRP -Plan de Recuperación de Desastres- y Continuidad TIC).
- RIESGO 2N.1 (Seguridad física de la TIC inadecuada).
- RIESGO 3N.1 (Controles inadecuados sobre el cambio o del desarrollo TIC).
- RIESGO 3N.2 (Arquitectura TIC inadecuada).
- RIESGO 4N.1 (Procesado o manejo inadecuado de TIC).
- RIESGO 4N.2 (Control inadecuado de los cambios a los datos en sistemas TIC en producción).
- RIESGO 5N.1 (Resiliencia inadecuada de terceras partes).
- RIESGO 5N.2 (Gobierno inadecuado de la externalización).
- RIESGO 1S.1 (Ciberataques disruptivos o destructivos).
- RIESGO 2S.1 (Ciberataques y otros ataques externos basados en TIC).
- RIESGO 2S.2 (Seguridad TIC interna inadecuada).
- RIESGO 3S.1 (Gestión inadecuada del ciclo de vida y el parcheado).
- RIESGO 4S.1 (Diseño inadecuado de los controles de validación de datos en sistemas TIC).
- RIESGO 5S.1 (Seguridad inadecuada de Terceras Partes).

Este mapa nos permite priorizar la gestión para reducir el riesgo tecnológico. Aquellos riesgos que se encuentran en la zona superior derecha deben ser gestionados con urgencia pues comprometen la supervivencia del negocio.

5.5- ANÁLISIS DE RIESGOS CRÍTICOS – PLAN DE ACCIÓN.

Este apartado recoge planes de acción que permitirán reducir la intensidad y/o frecuencia de los dos riesgos más importantes detectados en el mapa de riesgos anterior. Se exponen dos a modo de ejemplo, ya que habría que desarrollar al menos planes para todos los riesgos que se encuentran en la zona 'roja' del mapa.

Para la empresa Compotec los riesgos más relevantes son aquellos que tienen que ver con su cadena de suministro, ya que como era de esperar se trata de una empresa de retail en el que el movimiento de su stock es un aspecto básico para ofrecer una calidad de servicio cercana a la que ofrecen su principal competencia en este sentido los riesgos más relevantes son:

RIESGO 1S.1 (Ciberataques disruptivos o destructivos).

Como se comentaba los ataques denominados de DDOS (Distributed Denial of Services) son los más comunes en aquellas plataformas que utilizan las empresas que tienen una alta dependencia del canal de Internet. Existen mafias perfectamente organizadas que se dedican a la extorsión a este tipo de empresas, solicitando una cantidad de dinero a cambio de no saturar sus canales de venta o de servicio a sus clientes. A diferencia de otras empresas las empresas con una alta dependencia del canal Internet no pueden restringir este canal ya que entraría en conflicto con la prestación de servicio a sus clientes. Existen empresas y soluciones de tecnología que ofrecen servicios de limpieza de tráfico web que son capaces de identificar y aplicar medidas relativamente efectivas sobre el tráfico que llega a una página web, el precio es variable (por el tipo de solución y por el volumen de tráfico) y su implantación también es variable (en función de la complejidad de la empresa adquiriente y de la tecnología contratada) pero en el caso de Compotec una solución de mercado podría estar en la horquilla de 50.000€ a 100.000€.

Este plan de acción también incluye el plan de acción para el RIESGO 2S.2 (Seguridad TIC inadecuada) en el caso de indisponibilidad del servicio.

RIESGO 3S.1 (Gestión inadecuada del ciclo de vida y el parcheado).

El caso de la gestión adecuada del ciclo de vida y parcheado de los sistemas de información y el software implantado para Compotec es similar al caso del hotel expuesto anteriormente. No obstante, existe una cuestión de tamaño que provoca que los costes de aplicación estén apalancados, dado que la infraestructura de tecnología y su modelo operativo están directamente relacionados, y además dicha infraestructura es mucho mayor que en el caso del hotel. Es complicado determinar el coste exacto de un proceso

de implantación de parches, pero es previsible que la empresa tenga que implantar software específico de gestión de parches para realizar una implantación automatizada que permita generar economías de escala dado el tamaño de la infraestructura TI. Aunque es difícil de estimar con exactitud es posible determinar que tanto el software, como los procesos de gestión de las actualizaciones puedan estar entre una horquilla de 100.000€ a 200.000€.

No obstante, dada la fuerte dependencia tecnológica que tiene la empresa Compotec, la gestión de los riesgos asociados a la tecnología deberían estar recogidos dentro de una función continua. En particular los riesgos asociados a la seguridad de la información y los ciberriesgos deberían tener un capítulo específico dentro de la gestión del riesgo de la empresa a la lista de la matriz de riesgos. Un buen comienzo sería la identificación de esta necesidad por parte de la dirección y la definición e implantación de un Plan Director de Seguridad de la Información que determine de acuerdo con la misión, objetivos e intereses de la compañía:

1) La posición de riesgo deseable por la dirección que recoja las diferentes perspectivas y sensibilidades de los “stakeholders” (accionistas, socios comerciales, etc.).
2) Un plan de acción para alcanzar dicha posición de riesgo deseable.

Por ello, resulta altamente recomendable que este Plan Director lo lleve a cabo un equipo multidisciplinar que incluya los puntos de vista de los diferentes procesos críticos de negocio de la organización.

Dentro de este plan de acción se debería establecer la necesidad de implantar una organización de seguridad que establezca y mantenga la función de gestión del riesgo ciber desde un plano técnico, operativo y de gestión de acuerdo a las necesidades de la organización debidamente contextualizados.

6. CONCLUSIONES

Cualquier negocio hoy en día está comprometido por el uso de la tecnología. Como hemos podido analizar en el transcurso de este documento, incluso negocios cuyo 'core' no es la tecnología, pueden desaparecer por una gestión incorrecta de esta. El robo de información podría conllevar como consecuencias impacto regulatorio y económico, mientras que el incendio del hotel no tendría por qué conllevar un impacto regulatorio.

El mapa de riesgos es una herramienta que facilita la toma de decisiones. Permite tener una perspectiva de los riesgos de una organización, su estrategia y su orden de prioridad. El primer beneficio que obtenemos de su uso es la valoración de los riesgos - en nuestro caso tecnológicos - de una organización. Para esto hemos realizado un análisis de cada uno de ellos para acabar determinando su posible intensidad y su frecuencia. El segundo beneficio es que permite priorizar, en función de su importancia, su gestión.

Es recomendable una vez que se ha elaborado un mapa de riesgos su revisión periódica. Las organizaciones son cambiantes y el entorno también por lo que los riesgos modificarán su posición en el mapa. La puesta en marcha de muchas medidas de prevención deberían generar una mejora en el lugar en el que se ubican los riesgos.

Cada organización tendrá un mapa de riesgos específico en un determinado momento del tiempo. Dependerá del negocio, el modelo de gestión, de los controles que tenga implantados, del apetito al riesgo… En consecuencia, cada mapa debe realizarse a medida de cada organización.

No hemos pretendido desarrollar un mapa de riesgos válido para dos tipologías de negocio. Nuestro objetivo ha sido explicar, a partir del desarrollo y exposición de casos prácticos casos, cómo elaborar un mapa de riesgos tecnológicos, analizar este tipo de riesgos en un par de contextos y mostrar su utilidad.

Nos sentiríamos muy satisfechos si alguno de los lectores de este trabajo se cuestionara desarrollar un mapa específico para su organización.

PATROCINADORES AGERS

HERBERT SMITH FREEHILLS

PATROCINADORES ISMS FORUM

Realizado por:

AGERS - Asociación Española de Gerencia de Riesgos

ISMS Forum - Asociación Española para el Fomento de la Seguridad de la Información

MÁS INFORMACIÓN EN

www.agers.es

www.ismsforum.es