INSTITUTO TECNOLÓGICO HOTELERO

Estudio de Viabilidad Centro de Operaciones de Seguridad para Hoteles

(SOC Hotelero)

AEI Instituto Tecnológico Hotelero

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Índice

Introducción

¿Qué es un SOC?

Una solución con servicios centralizados que permiten la monitorización y respuesta inmediata ante incidentes, recogiendo la información de los sistemas conectados e interviniendo remotamente cuando es necesario, compuesto de un equipo de seguridad que supervisa la infraestructura TIC 24/7 para detectar en tiempo real cualquier incidencia en materia de ciberseguridad y reaccionar de forma rápida y eficiente.

Uno de los aspectos más relevantes de un SOC para un hotel es que no se trata únicamente de una plataforma de carácter reactivo, sino que un SOC también es responsable de la prevención, de la preparación y planificación de la estrategia de seguridad, su mantenimiento y preparación de rutinas de las medidas de seguridad establecidas como la realización de copias de seguridad, evaluaciones de vulnerabilidades, etc.

Por ello, es de vital importancia realizar este EV para definir un SOC adecuado por y para el sector hotelero, cuyos resultados sentarán las bases para del desarrollo efectivo de un SOC que pueda vigilar los riesgos de distintos hoteles de manera centralizada, logrando una mayor inteligencia de la información y de las amenazas generalizadas en los hoteles, beneficiando, por tanto, a todo el sector.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Objetivos EV

Objetivos principales del EV y específicos de la puesta en marcha del piloto

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

El SOC Hotelero se plantea como una herramienta con dos partes:

1. una centralizada, que permita a los hoteles conectados beneficiarse de una monitorización de las amenazas más avanzada y efectiva
2. una distribuida, que les permita dar respuesta según sus particularidades como organización y en el entorno tecnológico

OBJETIVOS ESTUDIO VIABILIDAD

- Dotar al sector hotelero de mayor conocimiento de los riesgos principales existentes en tiempo real.
- Mejorar la capacidad de prevención de ataques sobre el sector hotelero, limitando su impacto, probabilidad de éxito o frecuencia de ocurrencia.
- Ganar la fidelización y confianza de los clientes en su interacción digital con el sector.
- Mejorar la respuesta en caso de incidente, garantizando la resiliencia del sector.

OBJETIVOS PROYECTO PILOTO (MOCKUPS)

- Analizar y determinar la eficacia y aplicabilidad del SOC en materia de seguridad digital de los hoteles cumpliendo con los requisitos de seguridad y optimizando los recursos en este ámbito.
- Comprobar la utilidad de las funcionalidades del SOC con los agentes claves del sector.
- Mejorar la representación de los resultados proporcionados por el SOC de tal manera que contribuyan a dar una respuesta ante incidentes más rápida, que permita tomar decisiones informadas con agilidad a los hoteleros.
- Crear concienciación sobre los principales riesgos digitales del sector.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

¿POR QUÉ ESTOS OBJETIVOS DEL ESTUDIO?

Oleada de hackeos a hoteles para estafar a usuarios de Booking a través de su app

Una campaña de ciberataques contra los alojamientos suplanta su identidad en la plataforma y lanza intentos de phishing contra los usuarios

La cadena de hoteles low cost Motel One sufre un ataque de ransomware

El incidente ha derivado en una brecha datos que incluye las tarjetas de crédito de algunos huéspedes

Marriott tendrá que pagar 23,8 millones de multa por una brecha que estuvo activa cuatro años

Publicado el 3 noviembre, 2020 por Celia Valdeolmillos

Los fallos de ciberseguridad se pagan: sanción histórica para Marriott

El grupo de ransomware 8Base ha atacado con éxito la empresa española PortBlue Hotel Group. El grupo dispone de hoteles en Mallorca, Menorca y Astorga. Afirman haber robado pasaportes de los clientes, etc.

Rusia ataca a empresas turísticas españolas por el apoyo a Ucrania

Paradores, Riu, Majestic, Petit Palace, Only You, Catalonia Hotels & Resorts y Spain.info figuran entre las víctimas

Caos en Las Vegas por una oleada de ciberataques del grupo de jóvenes hackers 'la Araña Desordenada'

Multa de 30.000 euros a un hotel por escanear el pasaporte de sus clientes

europapress / andalucía

Suplantan la identidad digital de una directora comercial de hoteles en Granada y estafan más de 38.000 euros

- **El ransomware Play reclama un ataque a la cadena hotelera alemana H-Hotels**

La banda de ransomware Play se atribuyó la responsabilidad de un ataque cibernético en H-Hotels (h-hotels.com) que resultó en cortes de comunicación para la empresa.

July 13, 2023

Radisson Hotels Experiences Data Breach of Guest Information Related to MOVEit Vulnerability

La cadena de hoteles InterContinental sufre un ataque de ransomware

Los sistemas TI de la compañía han sido comprometidos, obligando a los hoteles a tomar las reservas por teléfono y a mano.

gmv

¿POR QUÉ ESTOS OBJETIVOS DEL ESTUDIO?

¿POR QUÉ ESTOS OBJETIVOS DEL ESTUDIO?

Fugas de información estratégica

Fugas de información de clientes

Perjuicio económico a clientes

Multas por incumplimiento de regulaciones

Impacto en las operaciones

Daño reputacional y pérdida de confianza clientes

Pagos no autorizados / Fraude financiero

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Acciones de investigación y consulta con el sector

Identificación de necesidades y valoración de la ciberseguridad

Procesos y metodología

Tipos de ataque como el "rasomware" el "mail del CEO", "phishing" o los ataques a páginas web y sistemas de gestión del hotel. Asimismo, se han identificado y analizado los vectores de ataque como las redes no segmentadas, la falta de seguridad en dispositivos y los softwares desactualizados, entre otros.

Focus Group sector alojamiento y Encuesta Ciberseguridad

Es necesario que toda la información sea validada por los agentes claves del sector, los que se beneficiarán del desarrollo de un SOC hotelero. Por tanto, todos los elementos analizados (amenazas, sistemas y dispositivos) y funcionalidades que podrían tener disponible el SOC, deben ser validades por los hoteleros y asociaciones quienes conocen las necesidades de sus establecimientos y asociados

Identificación y análisis de principales amenazas y riesgos digitales

Producto:
Guía Ciber-Riesgos para el sector hotelero

Identificación de necesidades, sistemas y dispositivos del sector a monitorizar por el SOC

Identificar qué sistemas y dispositivos pueden ser conectados a un SOC, validar con los hoteleros cuáles serían los más relevantes a monitorizar por un SOC e identificar las posibles barreras para desplegar un SOC sectorial

Análisis y presentación de funcionalidades

Las funcionalidades que puede tener un SOC pueden ser distintas según el sector, aunque haya elementos generales a monitorizar, dependiendo del tipo de alojamiento, pueden existir funcionalidades que solo sean de interés para establecimientos de gran tamaño y no para pequeños.

Contrastar con el sector y validar amenazas y funcionalidades

Diseño de piloto (mockups)

Finalmente, con la información recogida validada, se puede diseñar un modelo de SOC Hotelero, ajustándose a las necesidades del sector y con funcionalidades de interés y utilidad para ellos. Con este diseño, se inicia la fase del proyecto piloto, en este caso un piloto estático, que permitirá a los responsables de los alojamientos tener una visualización de cómo sería el SOC, su cuadro de mandos y para qué servirían las distintas funcionalidades incluidas.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Resultados fase investigación

MAYORES IMPACTOS DE CIBERSEGURIDAD

- Fuga de información del cliente
- Pagos no autorizados/fraude financiero
- Daño reputacional y pérdida de confianza del cliente
- Multa por incumplimiento de regulaciones

AMENAZAS EN CIBERSEGURIDAD MÁS PREOCUPANTES

- Phising e ingeniería social
- Ransomware
- Insiders maliciosos
- Ataques a sistemas críticos
- Mail del CEO

MAYORES DEBILIDADES DEL SECTOR

- Malas prácticas
- Sistemas desactualizados
- Falta de seguridad en los dispositivos
- Falta de monitorización y respuesta ante incidentes
- Falta de concienciación

PRINCIPALES ESCENARIOS DE RIESGO PARA HOTELES

- Phishing y ataques de ingeniería social en los que empleados o huéspedes son engañados por ataques de phishing, comprometiendo credenciales o información sensible
- Fuga de datos de clientes donde un atacante logra acceder a la base de clientes comprometiendo información personal y financiera
- Ataques a sistemas de reserva en línea, manipulando reservas o accediendo a información confidencial

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Resultados fase investigación (2)

VENTAJA MÁS INTERESANTE DE UN SOC HOTELERO

Conocimiento compartido (inteligencia): generar un conocimiento para todos los integrantes del sistema, compartiendo experiencias y situaciones que se hayan dado en un establecimiento hotelero y utilizando ese conocimiento para poder aplicar medidas y prevenir posibles incidencias en el resto de los integrantes del sistema

BARRERAS MÁS DETERMINANTES PARA DESPLIEGUE DE UN SOC

- Falta de personal especializado
- Presupuesto limitado
- Homogeneización de procedimientos
- Integración tecnológica

CASOS DE USO MÁS INTERESANTES PARA MONITORIZAR POR EL SOC

- Monitorización de la **infraestructura de red del hotel** en busca de signos de acceso no autorizado o actividades maliciosas: Patrones inusuales de tráfico de red, detección de malware o intentos de intrusión, dispositivos no autorizados en la red, etc.
- Monitorización de las **Plataformas de Reserva**: Intentos de acceso no autorizado a plataformas de reserva mediante ataques de fuerza bruta, detectar ataques DDoS que podrían afectar la disponibilidad de la plataforma de reservas.
- Monitorizar **transacciones y sistemas de pago** para detectar actividades fraudulentas: Patrones de transacciones inusuales, múltiples intentos de pago fallidos, acceso no autorizado a los sistemas de pago.

Guía de Ciber-Riesgos para el Sector Hotelero

Descárgate la Guía aquí:

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Propuesta técnica Piloto (Mockups)

Piloto estático diseñado en base al feedback recibido por el sector y evaluado por ellos.

Procesos para el diseño del piloto (Mockups)

Con los alojamientos y asociaciones interesados en formar parte del piloto, se celebra una primera reunión para explicar en qué va a consistir el piloto estático y se les explica en mayor medida qué es un SOC y cómo se incorporarían las funcionalidades identificadas de interés al SOC

Con todos los módulos presentados y explicados, se manda a los participantes del piloto un cuestionario de evaluación para recibir su feedback sobre su utilidad y satisfacción del futuro SOC Hotelero

Reunión Inicio del piloto

Presentación de mockups y validación de los módulos incluidos

Evaluación de Mockups por participantes del piloto

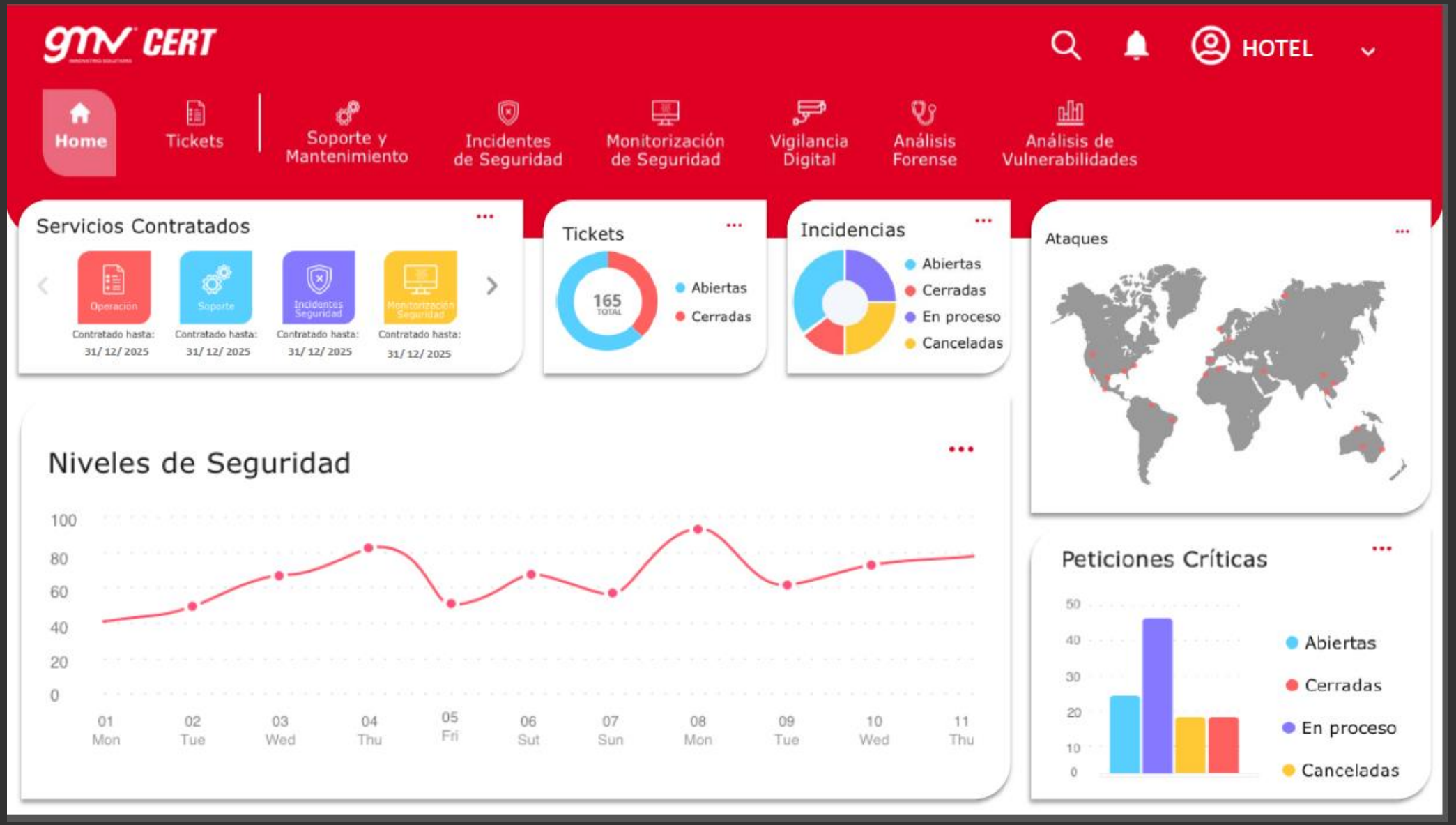
Diseño de la propuesta técnica final

Con todos los inputs, se diseñan los mockups, que presentan visualizaciones de cómo sería la parte visible (cuadro de mandos) del SOC, con los módulos (funcionalidades), con objeto de valorar su utilidad

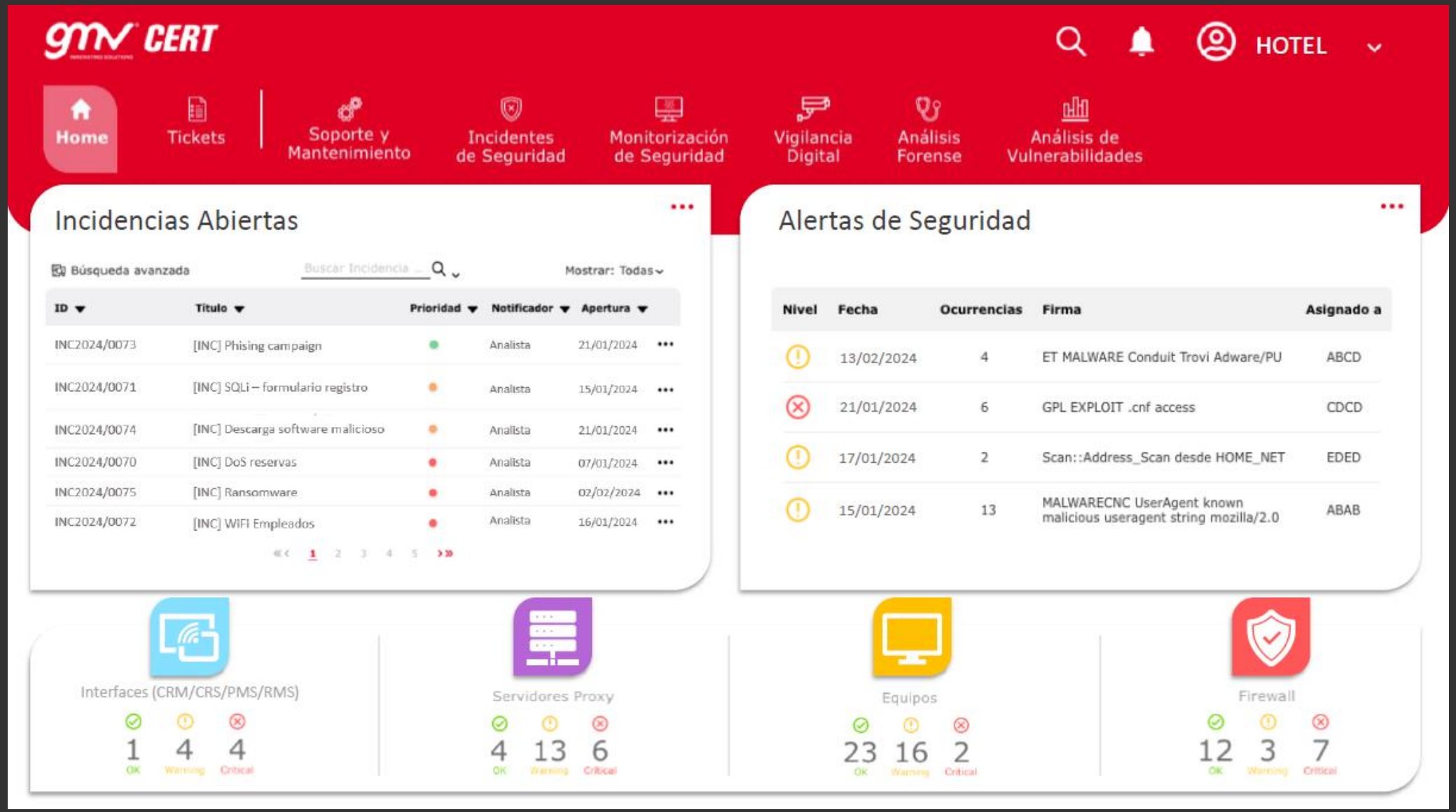
Recogido y evaluado el feedback, se puede tener un diseño final de la configuración del SOC para el sector hotelero, una propuesta que se ajusta a las necesidades del sector gracias a la colaboración ofrecida por ellos durante el piloto

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Piloto estático: Mockups SOC Hotelero

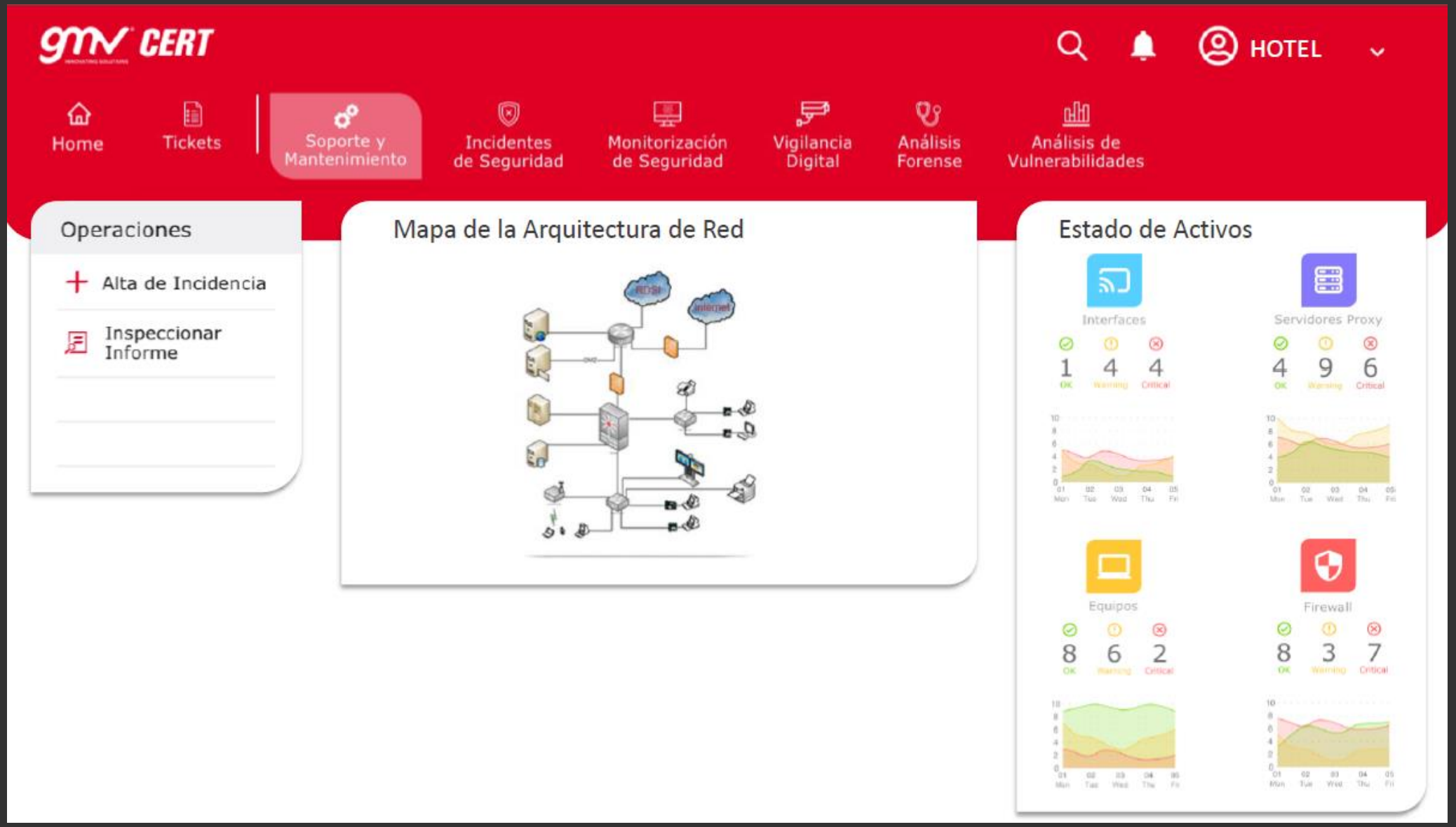


Piloto estático: Mockups SOC Hotelero

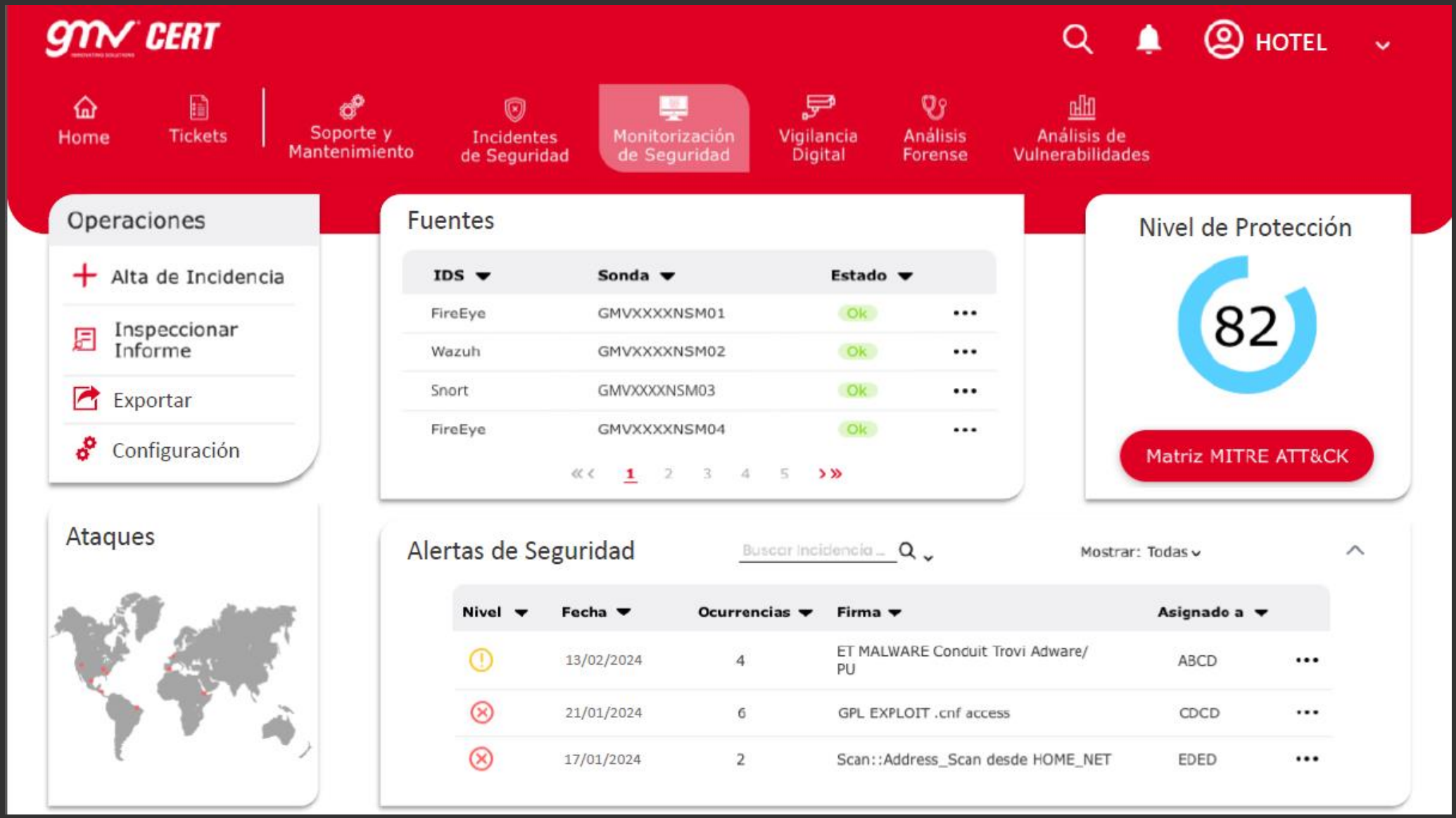


Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Piloto estático: Mockups SOC Hotelero



Piloto estático: Mockups SOC Hotelero



Valoraciones de los mockups del SOC Hotelero

- Existe **unanimidad** en la conveniencia de **monitorizar el PMS**.
- La mayoría de los participantes considera **conveniente monitorizar** los Channel Management Systems, CRM, RMS y OTAs.
- **Otros sistemas sugeridos para monitorizar**: Azure, O365, herramientas de servicios de terceros y CMS (Content Management System)
- **Buena acogida general** de las **funcionalidades** y vistas presentadas en el mockup.
- "**Incidentes de Seguridad**" y "**Monitorización**" son las vistas más valoradas del Dashboard.
- Todos los participantes muestran **interés** en que haya una **funcionalidad de análisis de vulnerabilidades.**
- La mayoría de los participantes considera interesante **incluir las funcionalidades avanzadas de vigilancia digital y análisis forense.**

Propuesta técnica de desarrollo SOC Hotelero

Operación

Prevención

Detección y respuesta

CERT Básico

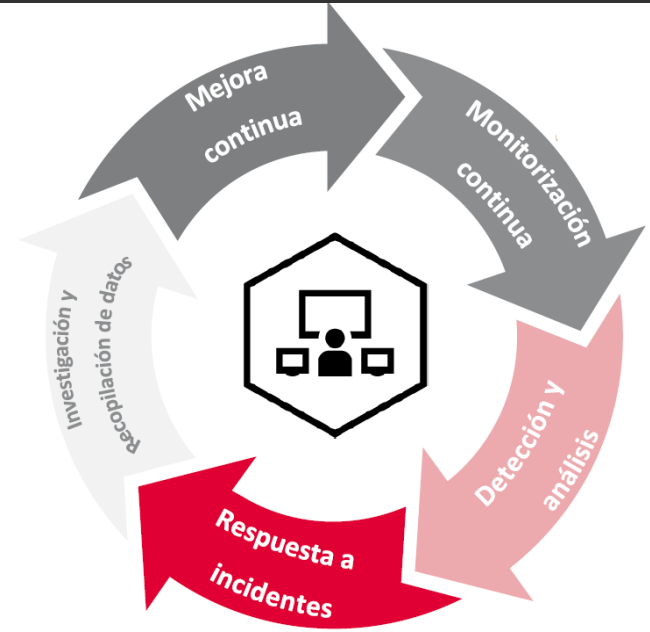
- Detección y Respuesta

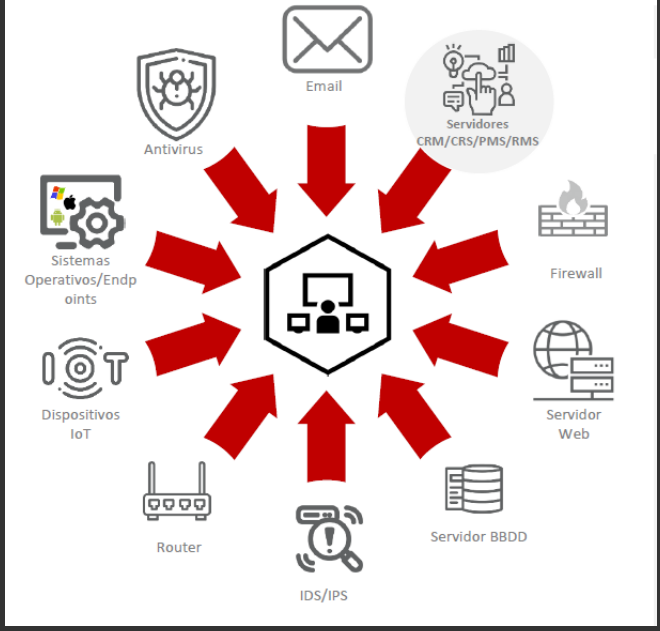
CERT Avanzado

- Detección y Respuesta
- Prevención
- Operación

CERT a medida

- Detección y Respuesta
- Servicios personalizados





Beneficios de utilizar un SOC en el sector

- Detección temprana de amenazas
- Respuesta rápida de eventos
- Protección proactiva
- Gestión centralizada de incidentes
- Recopilación y análisis de datos
- Cumplimiento normativo
- Confianza del cliente
- Gestión de la reputación

Conclusiones

Conclusiones del Estudio de Viabilidad

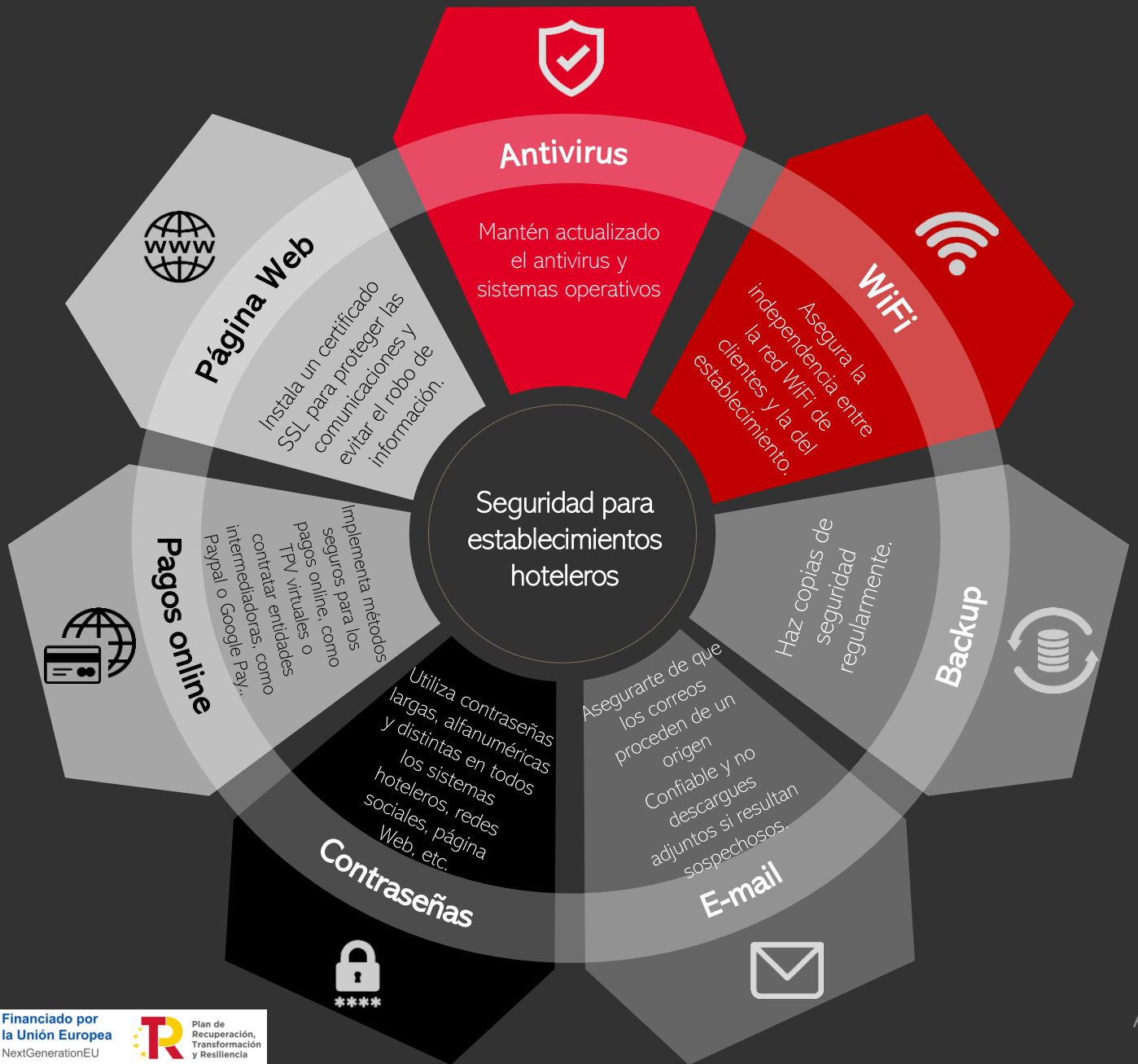
Conclusiones

- El diseño de soluciones tecnológicas efectivas para el sector requiere de una **colaboración por parte de los agentes del sector** que puedan valorar si la propuesta es de utilidad y de interés para la operativa del negocio antes de que estas soluciones salgan al mercado**.**
- No todos los alojamientos disponen de los mismos sistemas para su actividad, sin embargo, **todos los que tengan** son herramientas digitales **fundamentales** para la actividad (PMS, CRM, Channel Manager, RMS, etc.) con **información sensible** y, por tanto, **deben ser monitorizados** por el SOC.
- Es necesario disponer de **un departamento de IT** (interno o externalizado) con **conocimiento de medidas preventivas** y que ayude al alojamiento en el diseño de una **estrategia de ciberseguridad** acorde a la infraestructura del establecimiento y de las soluciones digitales de las que dispone.
- Pese a que el sector alojativo es objeto de numerosos ciberataques, aún **no hay una preocupación extendida** en los hoteles en este ámbito, **pocos** son los que **disponen de medidas preventivas eficientes.**
- Cuanto **mayor número de hoteles** se adhieran, **mayor será el conocimiento** compartido y **mejor preparados** se estará para hacer frente a los riesgos digitales del sector.
- El futuro desarrollo tecnológico de este SOC se plantearía con **distintas fórmulas de adhesión**, de forma que se ajuste a las diferentes tipologías de establecimientos y a sus **necesidades** concretas.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Recomendaciones finales

Recomendaciones de seguridad



Recomendaciones de seguridad

SEGURO CIBERHOTEL

ITH y GARCÍA ALAMÁN ponen en marcha un colectivo de compra abierto para el sector hotelero con el objetivo de generar una solución aseguradora que proteja a los establecimientos turísticos en su entorno digital. A este colectivo se podrán sumar cadenas hoteleras, hoteles independientes, apartoteles, hostales, alojamientos rurales y campings. Cuantos más seamos, mejores condiciones obtendremos.

¿POR QUÉ UNIRSE AL GRUPO?

- Obtendrás mejores condiciones económicas que contratando un seguro ciber por tu cuenta.
- Mejores coberturas: esta póliza contemplará las particularidades del negocio hotelero y alojamientos turísticos al contrario que las pólizas ciber genéricas.
- Ponemos a tu disposición y sin coste a nuestro asesor de confianza para resolver tus dudas, adaptar la póliza a tus necesidades particulares y orientarte en otras materias de aseguramiento.
- Aseguramos toda la actividad digital y online de tu negocio hotelero, aparthotel, hostal o camping.

¿QUÉ INCLUYE EL CIBERSEGURO?

- Extorsión cibernética
- Pérdida de datos
- Reclamaciones y multas
- Pérdida de beneficios

ÚNETE AL GRUPO EN:
CIBERSEGUROITH.COM

Gracias

Paula Miralles

pmiralles@ithotelero.com

www.ithotelero.com