handSIP by alhambra

OneseQ by alhambra

Minimiza los riesgos de tus clientes: apuesta por la Ciberseguridad as a Service

handSIP by alhambra

Servicios Seguros de Voz en la Nube para el Canal

Juan Bautista Rodríguez
Channel Manager HandSIP

Servicios Seguros de Voz que mejoran tus comunicaciones

handSIP by alhambra

SIP Trunk

Máxima calidad y ahorro de costes con nuestras líneas de Telefonía IP.

Centralita Virtual

Servicio profesional de centralita virtual avanzada sin límite de crecimiento.

Call Center

Convierte los puestos de los usuarios en auténticos puestos de Call Center.

Fax

Servicio de fax profesional de ámbito Internacional en modelo pago por uso.

SMS

Envío y recepción de SMS de manera sencilla desde tu correo electrónico o vía web.

Conectividad

Soluciones de comunicaciones diseñadas para la Pyme: ADSL/VDSL, FTTH, Fibra Dedicada.

WiFi Segura aaS

Servicio Wifi gestionado: análisis, diseño, oferta, implementación y monitorización/soporte.

Alhambra Cloud

Servicios seguros Cloud y MultiCloud que protegen tu negocio.

www.handSIP.com

OneseQ by alhambra

¿ Y Quién es Alhambra?...

El equipo humano de Alhambra que hay detrás de handSIP tiene una dilatada experiencia en proyectos y servicios a clientes, ya que es el Core del negocio desde su creación en 1991.

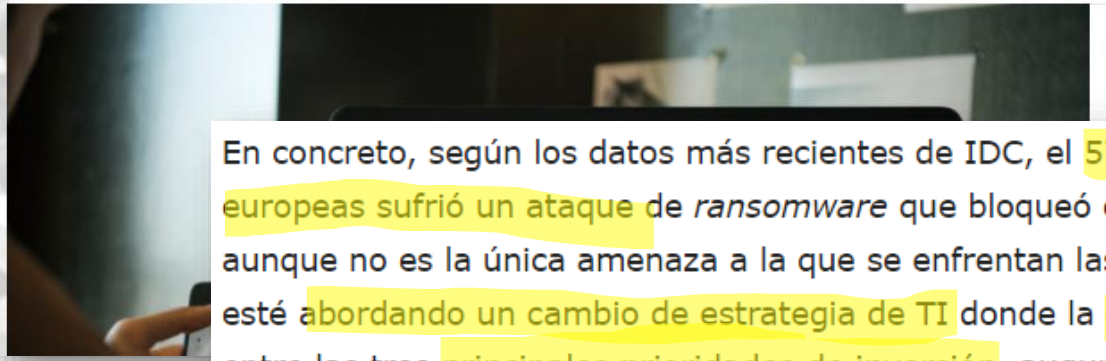
Formar parte de un equipo con una estructura consolidada nos permite dar los servicios actuales con SEGURIDAD.

“Seguridad Gestionada SECaaS, la clave del mercado”

Jose María Ochoa
Area Manager OneseQ | Cybersecurity

El mercado de ciberseguridad alcanzará los 1.749 millones de euros en España en 2022

28 de febrero de 2022



En concreto, según los datos más recientes de IDC, el 57% de las organizaciones europeas sufrió un ataque de *ransomware* que bloqueó el acceso a sus sistemas en 2021, aunque no es la única amenaza a la que se enfrentan las empresas. De ahí que el 90% esté abordando un cambio de estrategia de TI donde la ciberseguridad vuelve a situarse entre las tres principales prioridades de inversión, augurando que este mercado sobrepasará en España los 1.749 millones de euros en 2022, prácticamente un 7,7% más que en 2021. El sector que más crecerá en inversión en seguridad será la Administración Pública, con un 8,3%.

Identificación Oportunidad | EXISTE una necesidad

Por último, IDC Research España prevé que, en 2023, el 55% de las organizaciones asignará la mitad de sus presupuestos de seguridad a ecosistemas/plataformas de tecnologías cruzadas diseñadas para un consumo rápido y una seguridad unificada para impulsar la innovación ágil.

Fuente: IT Reseller

Prioridades de gasto

La encuesta muestra que el gasto se distribuye en varias áreas, **con un 20% asignado a infraestructura y hardware locales**, un 19% a personal cualificado, y un 16% a herramientas de software. A estas prioridades le siguen las soluciones de seguridad basadas en la nube, servicios de consultoría, servicios de monitorización basados en la nube, capacitación y concienciación, **servicios de evaluación contratados y servicios de respuesta a incidentes externos.**

Identificación RIESGO | EXISTE un problema

Las organizaciones enfrentan pérdidas masivas en incidentes

3MM

de empresas PYME y MicroPYME desprotegidas

4M€

Coste medio por incidente

60%

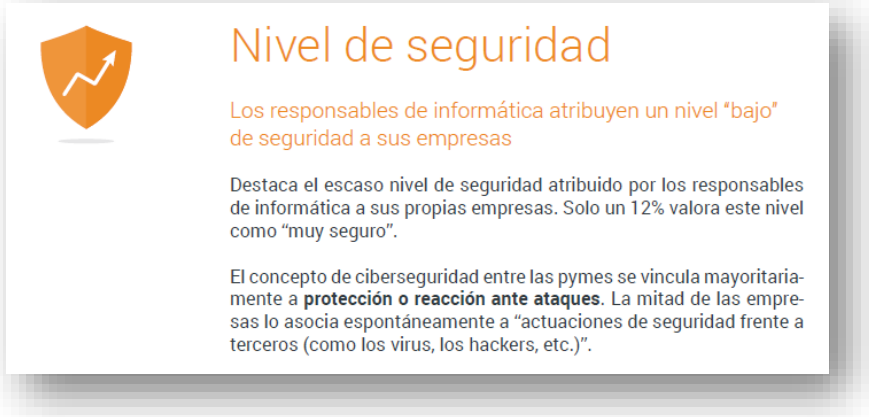
60% cierra seis meses después

- Tan solo un 36% de las Pymes tienen protocolo correcto de Ciberseguridad.
- Siendo un llamativo 70% como resultado directo de fraudes de ingeniería social.
- Además, el 70% empresas comunican erróneamente a los empleados la GDPR, y el 50% desconocen sus protocolos y sanciones.

Contexto | ¿Por qué es importante la defensa proactiva?

Actualmente, la mayoría de las compañías españolas tiene un **enfoque reactivo** sobre la seguridad IT de sus infraestructuras. Además, en el caso de utilizar fuentes de inteligencia, las empresas tienen una **información desfasada**, apenas fiable y por lo tanto poco práctica.

De manera que la **defensa proactiva basada en la información de riesgos** es una necesidad y un reto para las organizaciones. Desde OneseQ te ofrecemos el servicios en modo proyecto y gestionados que permiten el sincronismo necesario para que el ecosistema sea eficiente por su correcta **gobernanza.**



¿En qué consiste? | Gobernanza de servicios

La ejecución de proyectos y servicios gestionados en el ámbito de la ciberseguridad se basan en la **inteligencia de amenazas y la sincronía de la detección y respuesta,** y ésta genera a su vez genera las capacidades de: **conocer, comprender y perfilar a los atacantes** de manera que podamos anticipar y detectar nuevos impactos que escapan a nuestras soluciones defensivas. Tener **visibilidad y sincronía en los ámbitos de detección y gestión**, nos da las capacidades de actuar de modo temprano.

Según Gartner, la **inteligencia de amenazas** es el “conocimiento basado en la evidencia, incluyendo información de contexto, las implicaciones, y demás variables que giran en torno a una amenaza, peligro existente o emergente sobre los activos, y que se puede utilizar para la toma de decisiones”.

Recursos | Servicios GESTIONADOS

> El empresario centrado en SU NEGOCIO

En las pequeñas compañías, no es posible tener responsables de Ciberseguridad, ni soporte técnico de alta capacitación … los empresarios con micro-Pyme e incluso Pyme deben de dedicarse a la mejora de sus servicios y dejar en manos de compañías proveedoras la gestión de su TI y de su Ciberseguridad.

red seguridad

Los servicios gestionados de ciberseguridad aportan un modelo de protección externalizado, efectivo y eficiente, pero adaptado a la realidad y al negocio de cada empresa.

BASES | Pilares de Ciberseguridad

Bajo estos básicos hemos creado una completa estructura de servicios gestionados que aportan un verdadero valor añadido en el área de ciberseguridad.

Seguridad activa accesible desde la Nube.

Sobre nuestra plataforma CLOUD construimos servicios de seguridad activa.

Uno de los pilares de los servicios de **OneseQ** es aportar toda la experiencia que acumula en el entorno de seguridad y aprovechar las sinergias del propio servicio cloud de Alhambra para habilitar el concepto de Servicios de Seguridad en la Nube.

Seguridad activa accesible desde la Nube.

> FWaaS

El acceso a la modalidad Premium en la seguridad UTM de alto rendimiento para proteger las redes corporativas de cualquier posible amenaza, ataque o fuga de información gracias al servicio **FWaaS** de **OneseQ**, un servicio que ofrece la más amplia gama de funciones de red y seguridad del mercado, en modalidad de pago por uso. Flexibilidad y sencillez para consolidar tus servicios de seguridad.

> WAFaaS

Las organizaciones que utilizan aplicaciones web y conectan sus datos a Internet necesitan soluciones de seguridad específicas, ya que son especialmente vulnerables a todo tipo de amenazas: accesos no autorizados, inyecciones SQL, ataques de denegación de servicio, de scripts de sitios…

El servicio **WAFaaS** de **OneseQ** proporciona todas las herramientas necesarias para neutralizar fugas de datos y ataques contra infraestructuras informáticas. Además, facilita el cumplimiento de las normativas internas y sectoriales que regulan la protección de datos.

> Balanceo de las granjas Web y cifrado de las comunicaciones

ADCaaS se trata de un servicio de seguridad en la nube que protege las aplicaciones Web y permite que esa carga de trabajo se traslade de la CPU del servidor web a otro dispositivo que realice todo el cifrado y descifrado, liberando, así, al servidor web para otras tareas.

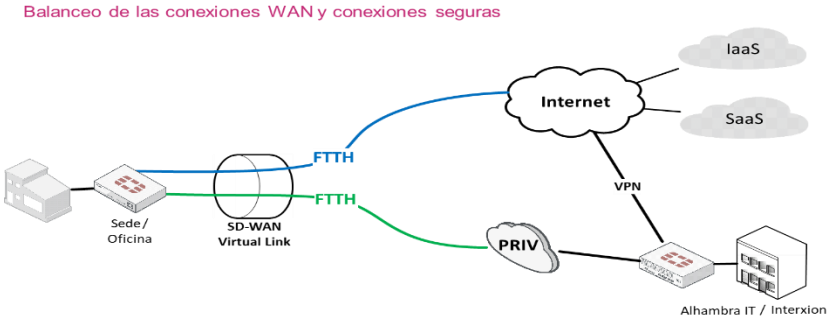
Seguridad activa accesible desde la Nube.

> NACaS

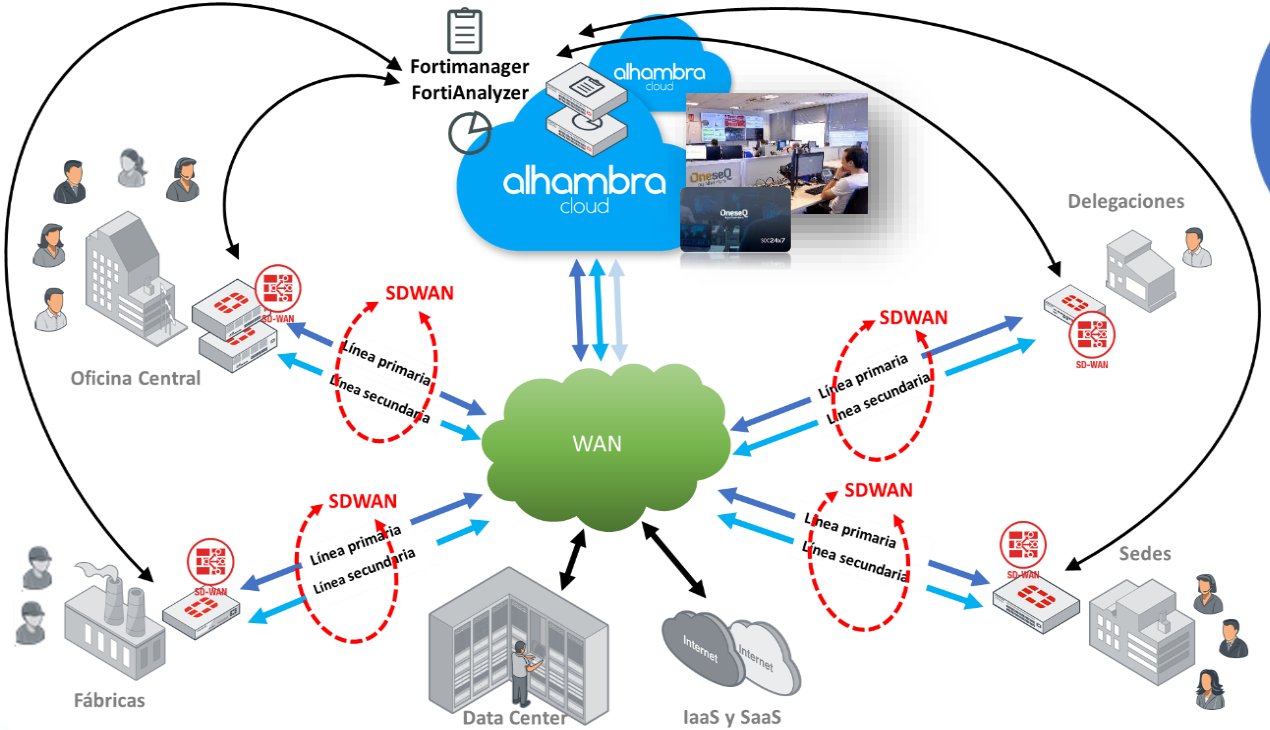
Adicionar capacidades de perfilado de usuarios para dotarles de permisos específicos dependiendo de parámetros del propio usuario o de la situación del mismo (localización geográfica, tipo de dispositivo, etc…) en el momento de conexión a recursos corporativos, nos aporta capacidades de defensa y detección más temprana.

> SDWAN_SEC

Generar redes de alto rendimiento en conmutación WAN pero dotándolas de la seguridad necesaria extendiendo el contexto global de seguridad definido en el core, hacia el punto local, y además integrarle el servicio gestionado de SOC | Alerta Temprana (monitorización, correlación y levantamiento de analistas) genera capacidades de gobernanza de seguridad que elevan las capacidades de protección pero también de recuperación.



Seguridad activa accesible desde la Nube.



Servicios de VALOR añadido
PROACTIVIDAD

Detectar – Pilar para desplegar contramedidas

Servicios gestionados SOC

Este servicio reúne los datos de los eventos, de las amenazas y de los riesgos para proporcionar la mayor información de seguridad, lograr respuestas rápidas a los incidentes

> Detección de intrusión

Es necesario un buen diseño de la interoperabilidad entre componentes de seguridad de los sistemas, así como de la correlación e inteligencia de los sistemas que estudian las actividades de los sistemas de la red.

> Monitorización activa de seguridad

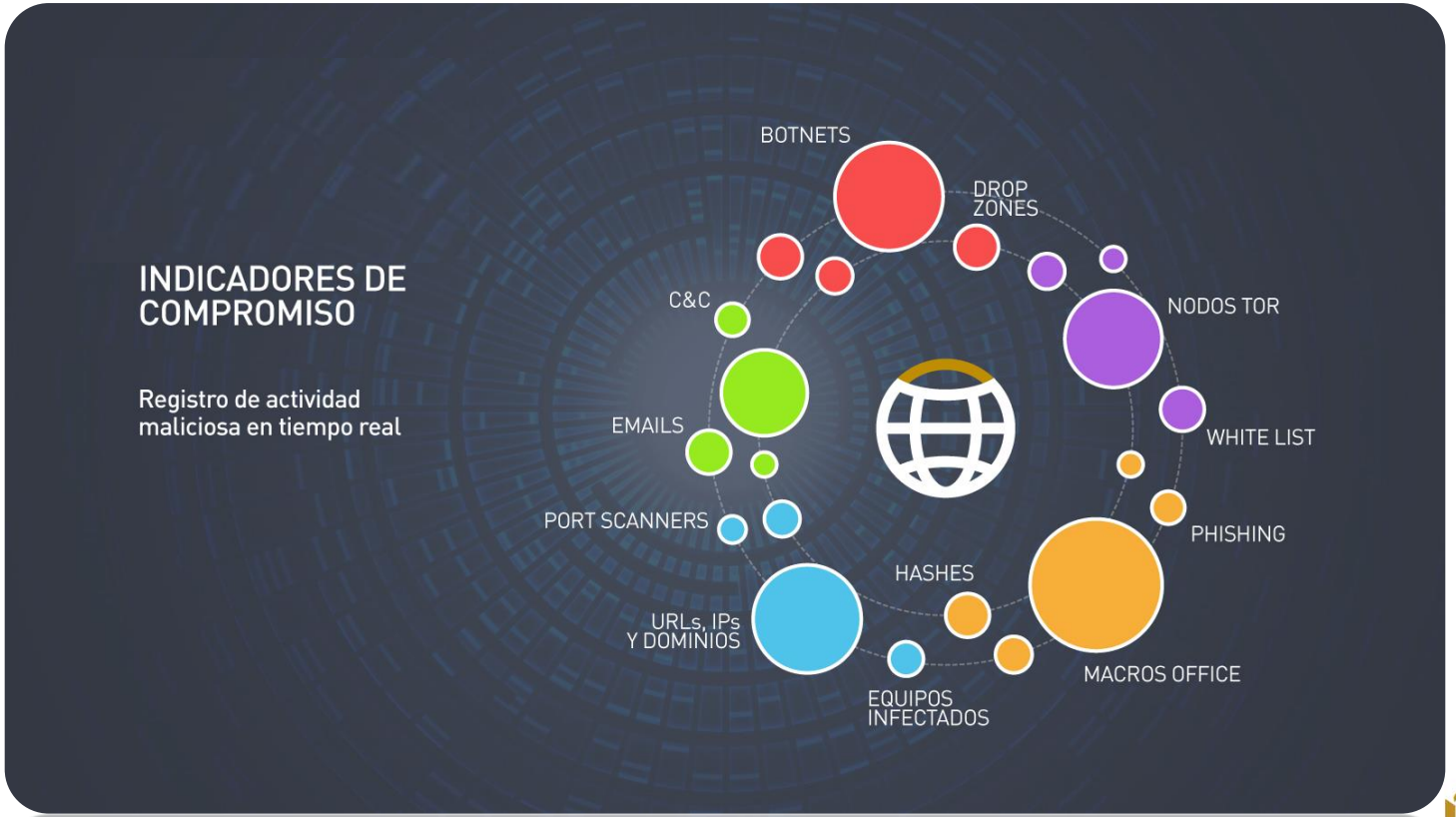
Este servicio reúne los datos de los eventos, de las amenazas y de los riesgos para proporcionar la mayor información de seguridad, lograr respuestas rápidas a los incidentes, gestionar los registros de forma sencilla y generar informes de cumplimiento ampliables.

La propuesta de OneseQ se focaliza en la consecución de los siguientes objetivos:

- ✓ Evolucionar los procedimientos y controles de seguridad de la organización
- ✓ Detección de amenazas contra los activos de la organización en tiempo real
- ✓ Capacidad para realizar investigaciones forenses y troubleshooting con un sistema centralizado donde se clasifique y estructure la información
- ✓ Generar indicadores de seguridad y negocio.
- ✓ Crear reglas complejas de correlación para detectar y generar amenazas avanzadas
- ✓ Disponer de dashboard y reporting a todos los niveles para disponer de información y conocimiento útil en todo momento.

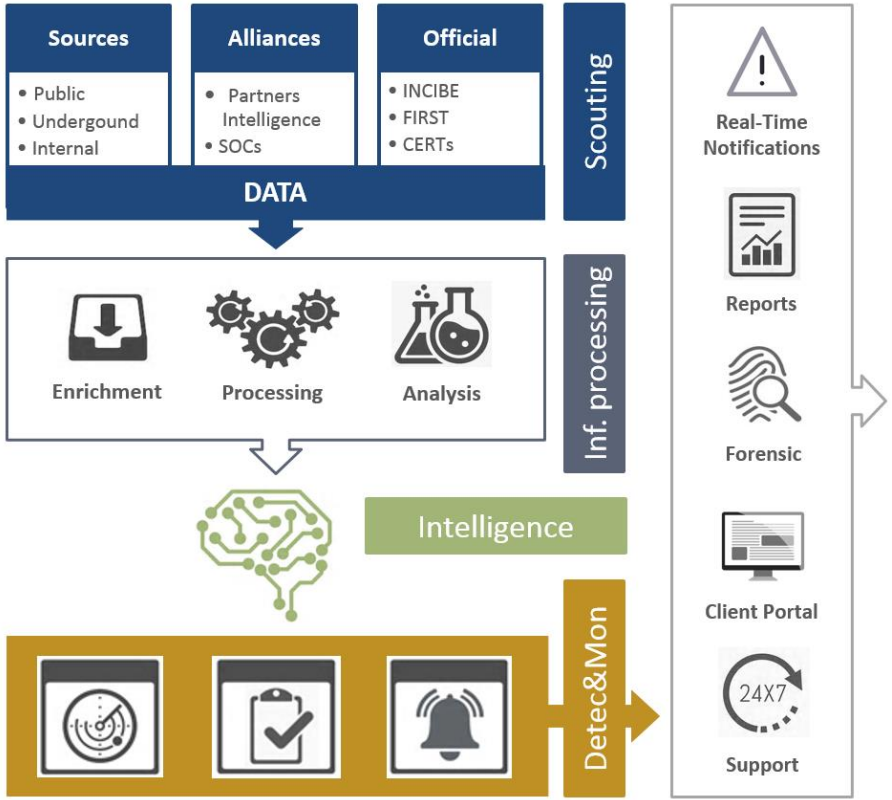
Añadamos algo adicional al conocimiento del riesgo

Conozcamos los recursos comprometidos



Pongámoslos en contexto (sepamos interpretarlos)

Funcionamiento | Alerta Temprana



Una vez la inteligencia es almacenada y procesada, el servicio SOC, lleva esta inteligencia a un **SIEM para realizar detecciones automatizadas y/o tareas de hunting**.

Con ello, también podemos automatizar algunas de las acciones de respuesta a incidentes mediante la **integración con otras plataformas y herramientas** (sistemas de tickets, cortafuegos, IDS, Sandbox, MISP, etc.).

Beneficios | SOC (Centro de Operaciones de Seguridad)

> Te ayuda a **conocer las amenazas externas e internas** a las que te expones.

> **Monitoriza** eventos e incidencias de seguridad

> Almacena eventos de seguridad como **evidencias para un posible forense**, proceso judicial, etc.

> **Previene posibles amenazas en el** futuro a través de la aplicación de las medidas **correctivas** correspondientes.

> **Genera mayor visibilidad sobre incidentes** de seguridad externos que pueden impactar en tus infraestructura.

> Evidencia la "**preocupación" por el control de la seguridad** de cara a normativa (GDPR, etc…)

Imagen de nuestro SOC (Madrid)

Servicios complementarios | OneseQ

Servicios gestionados desde el SOC

Una vez realizado e implantadas las medidas y contramedidas del plan de ciberseguridad, el cliente podrá incorporar **capas de servicios gestionados adicionales**, aportados por los analistas del SOC para dar valor a los sistemas de seguridad y así poder capacitarlas de **tecnologías de alto rendimiento y soporte especializado**, como son:

Una red de conocimiento | generación de VALOR

Objetivos

Desde la creación de **OneseQ** se marca como objetivo y valor complementario, la incorporación de la colaboración con centros y fuentes exteriores de información de cibervigilancia y cooperación entre SOCs mediante la generación de estrechas alianzas con un partner estratégico adicional con implantación de SOC, que brinda su apoyo y coordinación de los centros de operaciones internacionales, aportando visibilidad y fuentes de datos en todo el tránsito del servicio de alerta temprana de incidentes.

Colaboraciones

INCIBE

CCN

FIRST

APWG

ISMFORUM

APTAN

Acreditaciones

ISO 9001 ISO 14001

Una red de conocimiento | generación de VALOR

RED de SOC

SOC Propios y socios

Madrid

Brasil

Santa Cruz de Tenerife

SOC Colaboradores

Barcelona

Chile

Casa Blanca (Marruecos)

Dubai (Emiratos Árabes)

Riyadh (Arabia Saudí)

vCISO – CISO as a Service

Servicio vCISO

Disponemos de profesionales con gran experiencia en CiberSeguridad capaces de establecer estrategias, planes y de aplicar distintas metodologías de Seguridad

> Servicio vCISO

Bajo nuestro servicios se analiza los riesgos de la empresa y se asesora para establecer una estrategia de CiberSeguridad que se mantenga en el tiempo, proponiendo planes de acción y activando soporte técnico especializado con el objetivo de la seguridad de todos los aspectos de la compañía.

Con todo esto uno de los puntos cruciales del servicio VCISO es la implantación de la" cultura de ciberSeguridad" en la organización, y para ello se genera una dinámica de concienciación en seguridad en todos los empleados y departamentos de la organización.

- ✓ Ayuda y definición de la estrategia de CiberSeguridad
- ✓ Generación de Borrador del Plan de Ciberseguridad de la compañía
- ✓ Gestión de Riesgos de CiberSeguridad
- ✓ Gestiíon de "Servicios implantados de ciberseguridad"
- ✓ Cumplimiento Normativo
- ✓ Concienciación en CiberSeguridad

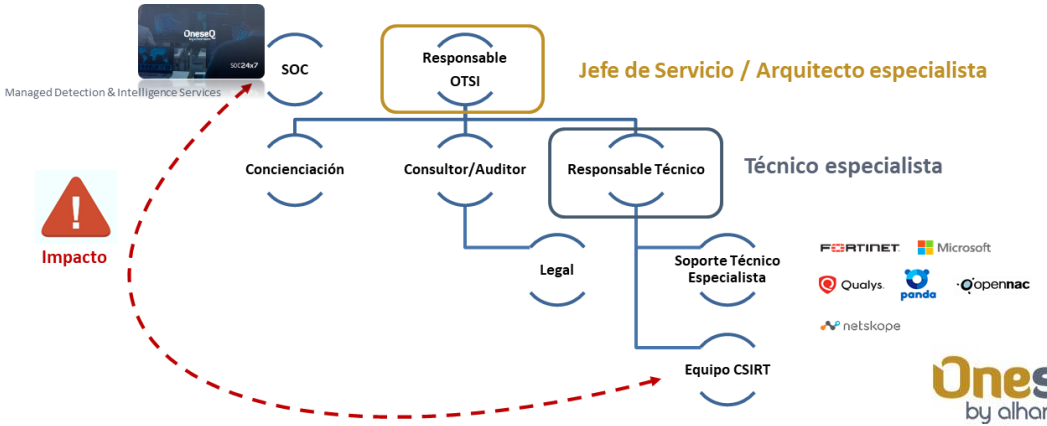
vOTSI – Oficina técnica de seguridad de la información

Servicio vOTSI

Disponemos de profesionales con gran experiencia en CiberSeguridad capaces de establecer estrategias, planes y de aplicar distintas metodologías de Seguridad

> vOTSI

La Oficina Técnica de Seguridad de la Información (OTSI) es una entidad "virtual" en la organización IT cuyo fin es proporcionar al cliente el servicio de soporte técnico adecuado en el ámbito de la ciberseguridad abarcando desde la definición estrategia hasta la implantación de las políticas, procesos y procedimientos que permitan al cliente conseguir los niveles adecuados de integridad, confidencialidad y disponibilidad que aseguren su continuidad operacional y servicios.



vOTSI – Oficina técnica de seguridad de la información

Servicio OTSI

Disponemos de profesionales con gran experiencia en CiberSeguridad capaces de establecer estrategias, planes y de aplicar distintas metodologías de Seguridad

- Ayuda en la definición de planes directores.
- Apoyo en el desarrollo y puesta en marcha de políticas y procedimientos de seguridad.
- Revisiones periódicas de aplicaciones y sistemas, y su configuración.
- Coordinación de proyectos de implantación de tecnologías de ciberseguridad.
- Coordinación de Soporte técnico especializado en proyectos de migración y/o puesta de marcha en marcha de nuevos servicios e infraestructuras.
- Coordinación de acciones de mejora de los niveles de seguridad del personal (formaciones técnicas, sensibilización, simulacros, etc.).
- Seguimiento de monitorización de los sistemas de información (alertas y gestión de incidentes).
- Seguimiento de acciones para la remediación de debilidades detectadas en impacto (CSIRT) como leves.

Otros servicios

Pleno rendimiento: Servicios de Seguridad.

> Servicios AUDIT SEC

Análisis y gestión de sistemas para identificar y corregir las vulnerabilidades que pudieran presentarse en las estaciones de trabajo, redes de comunicaciones o servidores.

> Test de Vulnerabilidades e Intrusión

Realizado como método de auditoría para intentar acceder a los sistemas y así comprobar el nivel de resistencia a la intrusión no deseada.

> TEST resistencia al Phishing (Phishing Fake)

Realice la simulación de cientos de ataques de phishing realistas y desafiantes en tan solo unos clics.

> Monitorización activa de seguridad SIEM/SOC – Alerta Temprana

Este servicio reúne los datos de los eventos, de las amenazas y de los riesgos para proporcionar la mayor información de seguridad, lograr respuestas rápidas a los incidentes, gestionar los registros de forma sencilla y generar informes de cumplimiento ampliables.

> Servicio vCISO

Disponemos de profesionales con gran experiencia en CiberSeguridad capaces de establecer estrategias, planes y de aplicar distintas metodologías de Seguridad

> Seguridad activa accesible desde la Nube

Sobre nuestra plataforma CLOUD construimos servicios de seguridad activa.

Identificar – base de los servicios de Ciberseguridad.

Auditoría de Seguridad

Análisis y gestión de sistemas para identificar y corregir las vulnerabilidades que pudieran presentarse en las estaciones de trabajo, redes de comunicaciones o servidores.

> Auditoría de seguridad IT (Descubrimiento de postura de seguridad)

El principal objetivo es el desarrollo de estrategias de protección de sus infraestructuras focalizadas en optimizar el uso de los recursos de seguridad, para lo cual se ejecutarán actividades metodológicas para la **identificación, clasificación y valorización** de los activos de configuración de la arquitectura de seguridad.

Además, se considerará la asignación de responsabilidades sobre el tratamiento de los servicios y activos críticos, permitiendo mantener claramente identificadas las necesidades de medidas y controles de seguridad sobre los activos de información relevante para EL CLIENTE y establecer en nivel de exposición a **los riesgos que representan las cyber amenazas.**

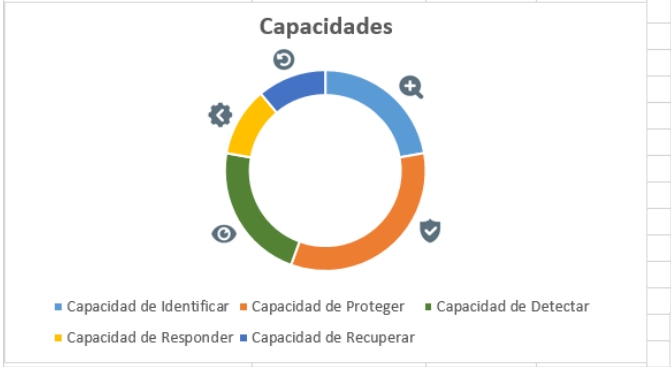
El alcance establecido para esta **fase de la consultoría** persigue definir y establecer:

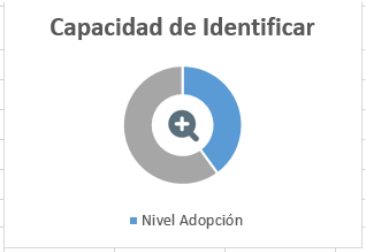
- ✓ **la Seguridad en el Acceso a la Información.**
- ✓ **la Optimización de la Gestión de Activos de Información.**
- ✓ **la Optimización de la Seguridad en las Comunicaciones y Operaciones.**
- ✓ **Enfoque y propuesta para: Modelo de Organización centrado en la Seguridad de la Plataforma de cada CLIENTE.**

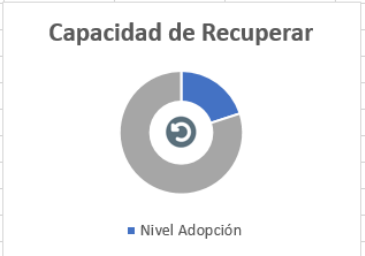
En esta fase se aplicará un **método de evaluación inductivo** centrado en las prácticas de EL CLIENTE, contra los mejores estándares de gestión de seguridad avanzada, con una metodología basada en **procesos aprendidos** en base a las **mejores prácticas** de la industria, para diseñar e implementar estrategias de Ciberseguridad.

Identificar, proteger, detectar, responder, recuperar.

Concepto	Nivel Adopción	Resto	Total
Capacidad de Identificar	2	3	5
Capacidad de Proteger	3	2	5
Capacidad de Detectar	2	3	5
Capacidad de Responder	1	4	5
Capacidad de Recuperar	1	4	5







Identificar – base de los servicios de Ciberseguridad.

Test de Vulnerabilidades

Realizado como método de análisis para verificar el estado de “salud” y parcheo de los sistemas de la infraestructura IT

> VAK (Test de vulnerabilidades)

El principal objetivo que se persigue es detectar e identificar de forma las posibles vulnerabilidades en los sistemas y servicios en producción y en los elementos de configuración que actualmente están vinculados o directamente relacionados a éstos y puedan ser accesibles o posibilitar el acceso a otros aplicativos y propicien una situación de riesgo no deseado.

Mediante la aplicación de las pruebas del test de vulnerabilidad perseguiremos los siguientes puntos:

- ✓ **Mitigar los posibles** riesgos de afectación de la plataforma tecnológica que soporta sus servicios identificando previamente la mayor cantidad de vulnerabilidad a que está expuesta.
- ✓ **Vislumbrar** los mecanismos reales y aplicables necesarios para corregir siempre y cuando estos no afecten el buen funcionamiento y disponibilidad de la plataforma tecnológica.
- ✓ **Identificar** otros tipos de pruebas de intrusión que puedan ser aplicables de acuerdo con la plataforma tecnológica existente, los resultados de las pruebas y el conocimiento y experiencia de OneseQ.

Identificar – base de los servicios de Ciberseguridad.

Test de Intrusión (Pentest)

Realizado como método de auditoría para intentar acceder a los sistemas y así comprobar el nivel de resistencia a la intrusión no deseada.

> PenTest (Red TEAM)

El objetivo que se persigue es posicionarse en el roll de atacante intentando “enumerar” (descubrir) vulnerabilidades y estado de salud de la infraestructura para hacer una explotación de las mismas y conseguir una penetración a los sistemas IT de la compañía cliente.

Hay varios tipos de Pentest, según la información de la que se tenga acceso:

- ✓ **Caja NEGRA** , el ethical hacking se realiza sin ninguna información adicional del cliente.
- ✓ **Caja GRIS** el ethical hacking se realiza con cierta información adicional del cliente, que puede dar permiso a ciertos recursos y así evitar la explotación por fuerza bruta, etc …
- ✓ **Caja BLANCA** el ethical hacking se realiza con mucha información adicional del cliente, como users y password privilegiados, etc …

Identificar – base de los servicios de Ciberseguridad.

TEST resistencia al Phishing

Realice la simulación de cientos de ataques de phishing realistas y desafiantes en tan solo unos clics.

> TEST resistencia al Phishing (Phishing Fake)

Los usuarios finales son el blanco más importante y vulnerable en la mayoría de empresas. En ataques del mundo real, los usuarios se ven constantemente bombardeados con timos de ingeniería social y suplantación de identidad selectiva.

Realice la simulación de cientos de ataques de phishing realistas y desafiantes en tan solo unos clics. Nuestros analistas monitorizan millones de mensajes de correo electrónico, direcciones web, archivos y otros datos que llegan a diario en busca de las amenazas más recientes. Este flujo de información constante garantiza que la formación de los usuarios comprenda tácticas de phishing actuales con plantillas de simulación de ataques socialmente pertinentes y abarque varios escenarios desde principiante a experto.

- ✓ **Testea y controla "el eslabón más débil de la cadena":** el usuario.
- ✓ **Reduzca la superficie expuesta a ataques** más amplia de su empresa: los usuarios finales.
- ✓ **Hagamos simulaciones de las brechas** más comunes y centrémonos en el eslabón más débil; el usuario.

¿Qué preguntar?

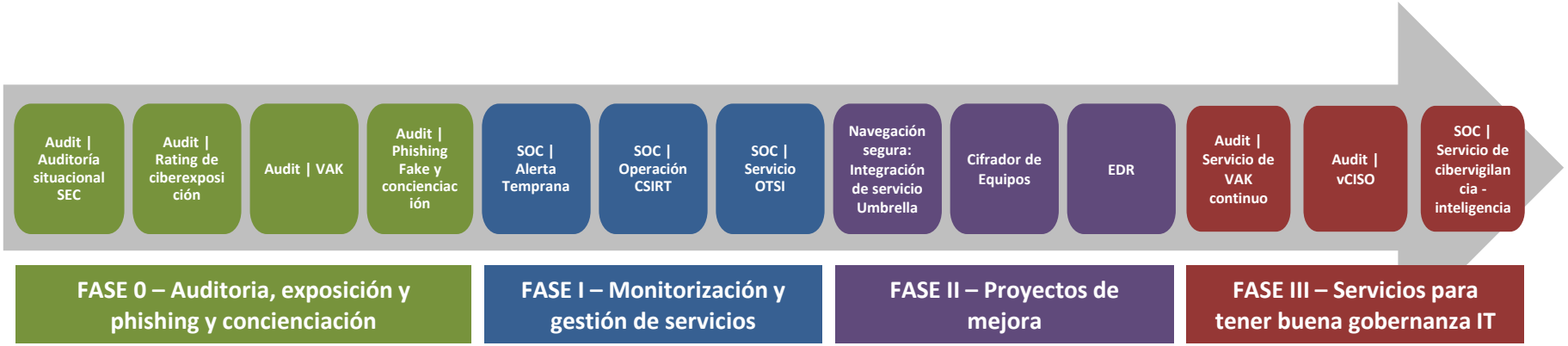
Preguntas base

- ¿Tiene su compañía departamento específico de seguridad IT (CISO, etc …)?
- ¿Han desarrollado un Plan Director de Seguridad?
- ¿Tienen identificados los activos de riesgo?
- ¿Implementan alguna buena praxis en la gestión de prevención de incidentes?
- ¿Qué controles del perímetro tienen implementados?
- ¿Qué técnicas de control de información implementan para evitar fuga y mala praxis?
- ¿Pasan regularmente auditorías de seguridad?
- ¿Tienen servicios en nube?¿Cómo capacitan su control?
- ¿Implementan en sus sistema recursos de recuperación ante desastres DRP?
- ¿Dicho DRP implementa niveles de seguridad IT similares a los activos?
- ¿Su plataforma de aplicaciones Web (Intranet, etc…) es controlada de algún modo?

Securización sistemas CLIENTE | Descripción

A continuación expondremos el plan, que desde OneseQ hemos configurado, para ir elevando los niveles de madurez en la gobernanza de la seguridad de los sistemas de **CLIENTE**.

La idea principal, es empezar cubriendo las necesidades más básicas e ir creciendo paulatinamente. Por ello creemos que el escenario más adecuado a este proyecto esta basado en varias fases:



www.handSIP.com | www.OneseQ.es