qualoom

¿Conoces el nivel de madurez de tu organización en material de Seguridad?

Área de consultoría tecnológica

01/01/2022

Aviso de confidencialidad

El presente documento es propiedad de Qualoom Expertise Technology S.L (en adelante Qualoom) y queda prohibida la reproducción total o parcial de la información contenida en el, así como su transmisión, cesión o alquiler mediante cualquier medio tanto analógico como digital.

La información contenida en el documento es de carácter confidencial. Qualoom y las personas o entidades a las que se distribuye, se comprometen a no revelar directa o indirectamente a terceros ajenos al proyecto la información contenida en el documento, sin el consentimiento por escrito de ambas partes.

Los servicios a realizar por Qualoom en las instalaciones o sistemas del Cliente no conllevan, necesariamente en sí mismos, el acceso a datos de carácter personal, y en ningún caso el tratamiento posterior de información de esta naturaleza. Por lo tanto, estos servicios no se encuadran exactamente en la figura de "encargado del tratamiento" establecido en el artículo 3 de la Ley 15/99.

No obstante, en cumplimiento del artículo 83 del Real Decreto 1720/2007, Qualoom, formalmente declara que el personal a su cargo ha sido suficientemente instruido en la prohibición de acceder a los datos de carácter personal y la obligación de secreto respecto a los datos que dicho personal hubiera podido conocer con motivo de la prestación del servicio .

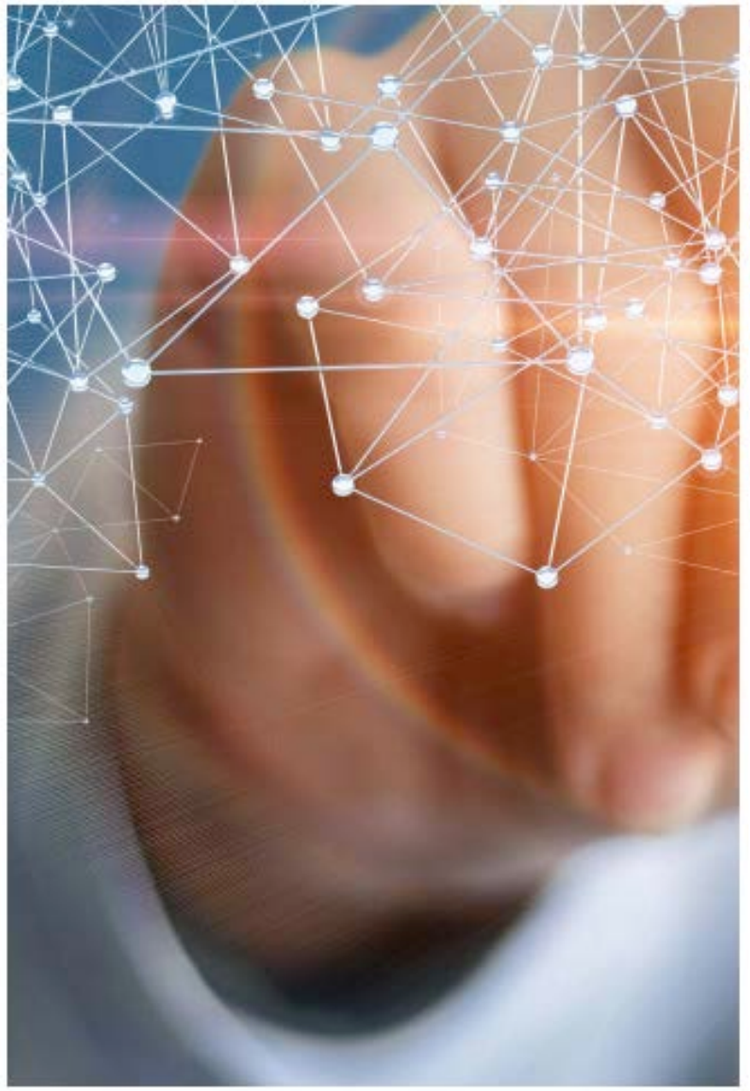
A los efectos de lo que dispone la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el signatario queda informado que los datos personales que nos facilite podrán ser incorporados a los ficheros mantenidos por Qualoom, en el ejercicio de su actividad.

Queda informado de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación u oposición a que haya lugar sobre dichos datos por correo electrónico a info@qualoom.es.

La seguridad en la organización

La seguridad de la información es todo el conjunto de técnicas, tareas, procedimientos, estándares, sistemas, software y acciones que se implementan para supervisar, analizar, controlar y mantener el estado de los activos de una organización en el estado original para el que fueron creados, velando por su correcto uso, integridad, disponibilidad y accesibilidad.

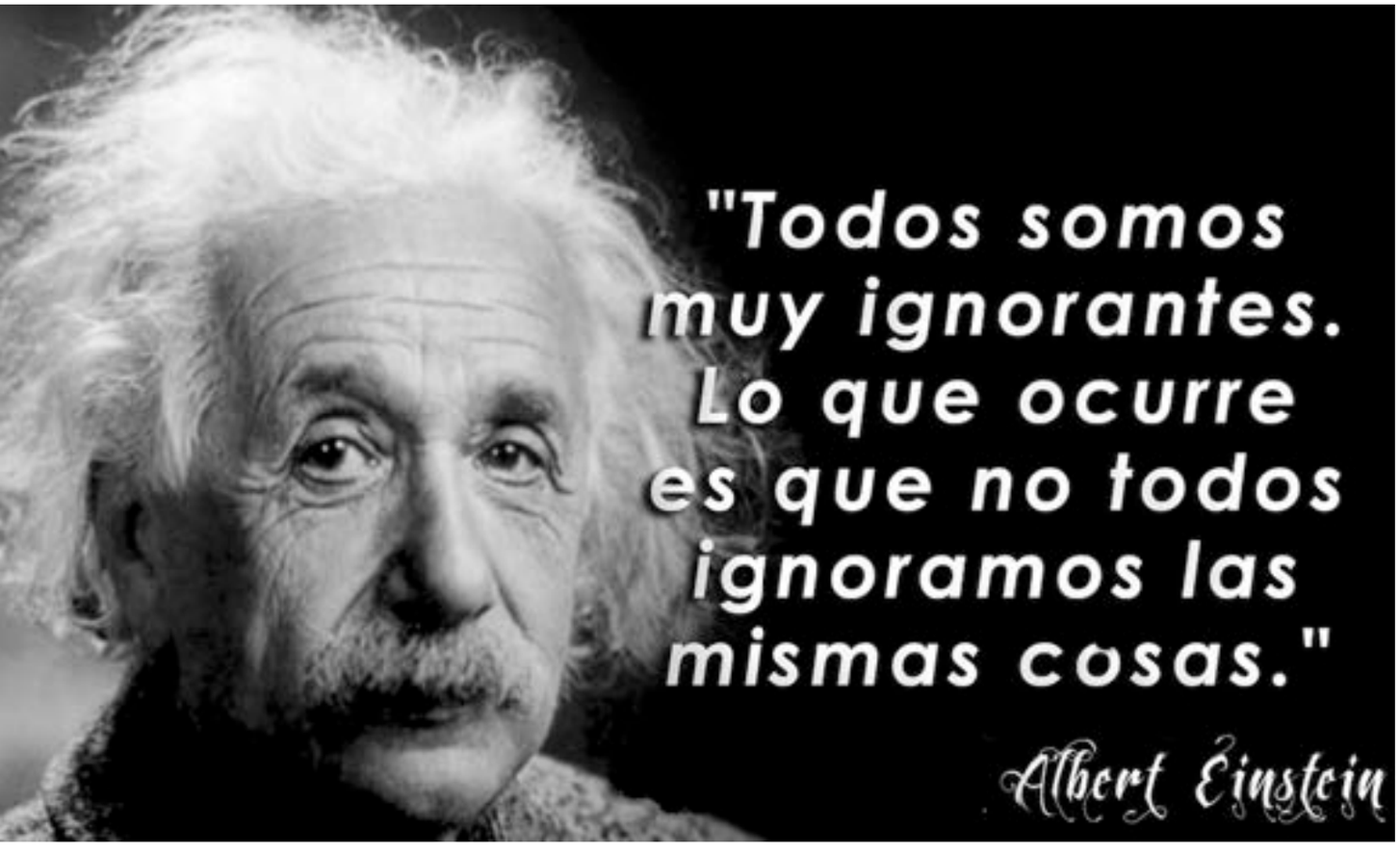
Bajo esta definición te invitamos a iniciar una viaje de autodiagnóstico que te permitirá conocer el nivel de madurez en el ámbito de la seguridad de la información de tu organización y los pasos que deberás dar para alcanzar un compromiso entre el tipo de actividad que desarrolla tu organización y los recursos de los que dispones.



«Una cadena es tan fuerte como su eslabón más débil

«El usuario es el eslabón más **IMPORTANTE** de la cadena de la seguridad»

¿Estas dispuesto a no conocer las amenazas que acechan a tu organización?



En muchas ocasiones, el no conocer las amenazas, riesgos existentes y el estado de tu organización es el mejor escenario para sentir seguridad.

Pero esta situación conlleva un grave riesgo y es el caldo de cultivo para sufrir los perjuicios irreparables de brechas de seguridad, pérdida de datos por virus, ransomeware, ataques de denegación de servicio, parada de servicios y otros muchos riesgos materializados de manera repentina.

¿Cuenta tu organización con áreas de responsabilidad en el ámbito de la seguridad?

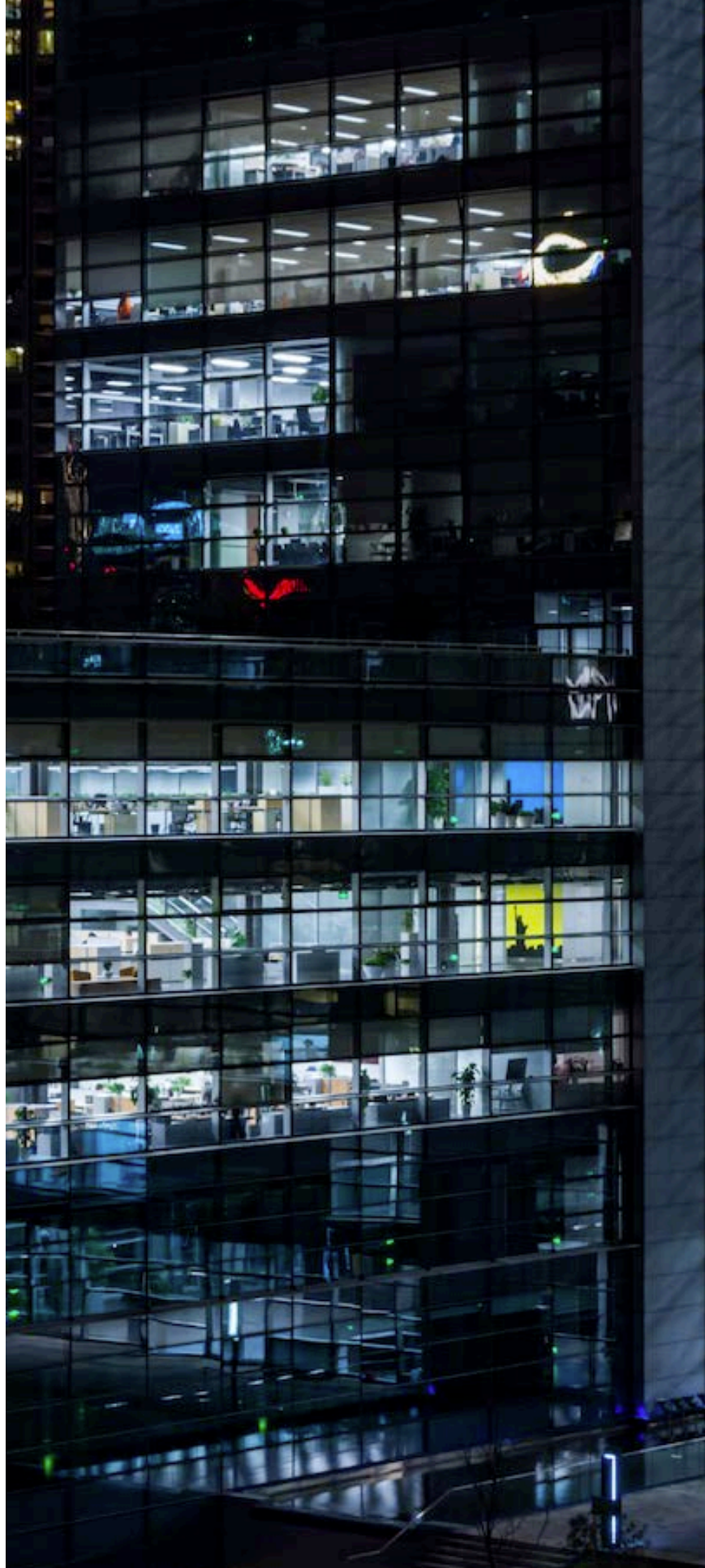
El primero de los pasos en el camino para alcanzar un adecuado nivel de seguridad, es la definición de **áreas de responsabilidad** lideradas por perfiles adecuados. La atribución de competencias en las citadas áreas de responsabilidad de una organización es la base fundamental para la correcta implementación de los mecanismos, procedimientos, aplicación de herramientas y métodos para la supervisión de cada uno de los activos implicados en la operativa diaria.

Para ello es fundamental:

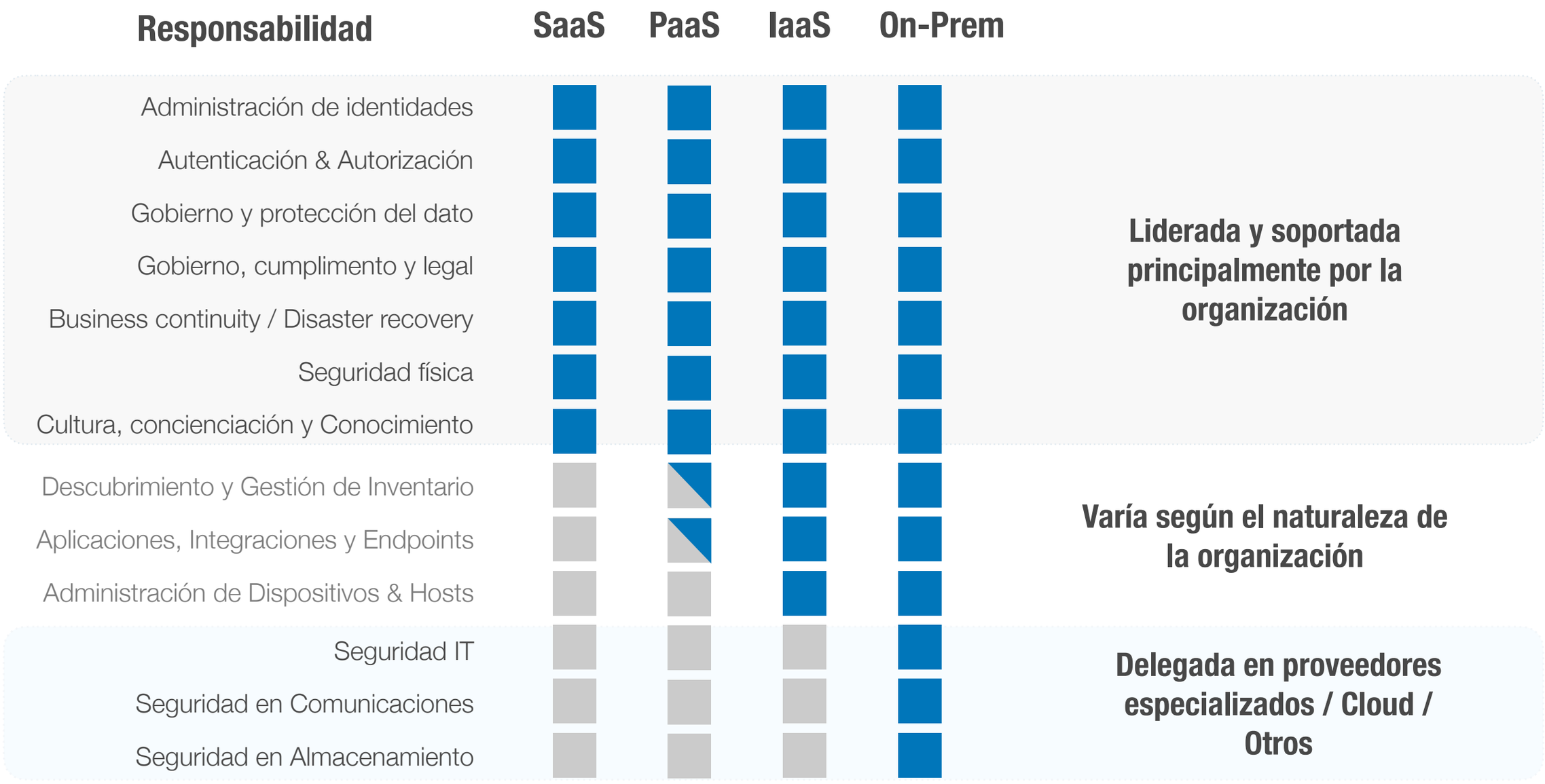
Definición de áreas de responsabilidad

Identificación de lideres de área

Atribución de responsabilidades y competencias



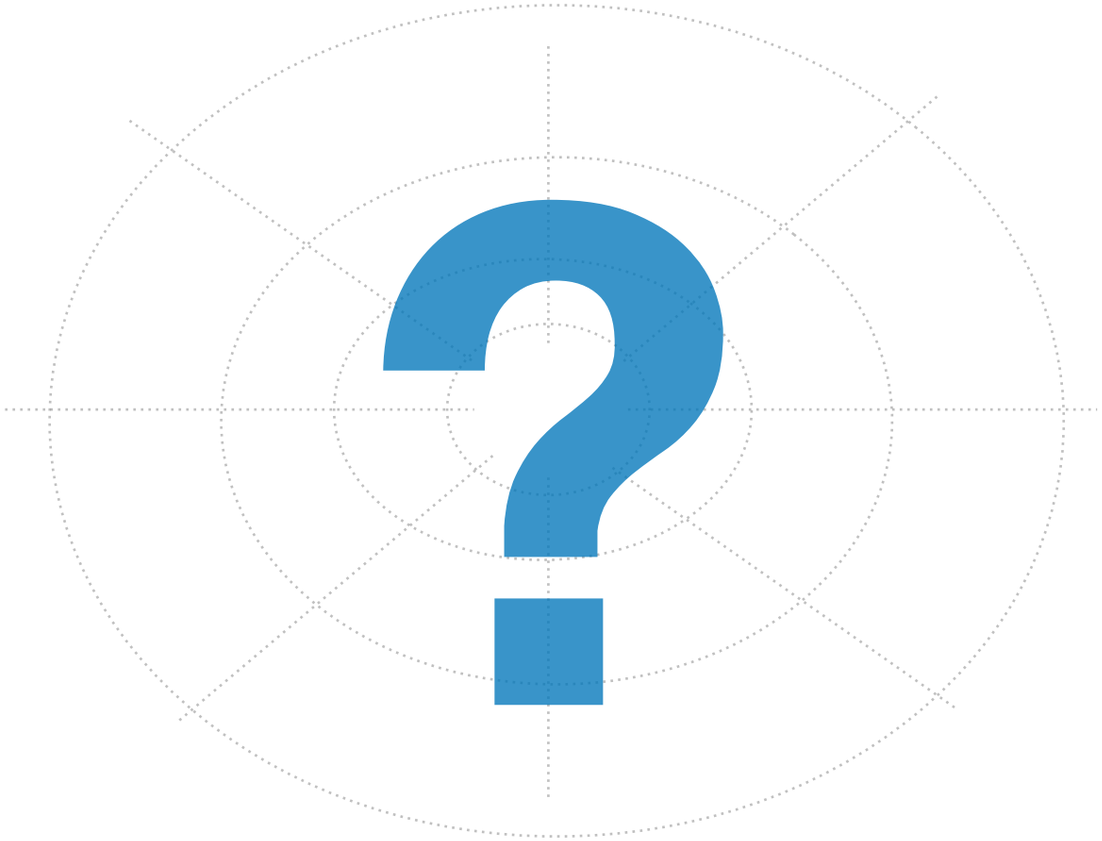
Te presentamos las áreas de responsabilidad esenciales en materia de seguridad



Identificación de relevancia en el cuadrante de criticidad

¿Te atreverías a situar en el cuadrante de criticidad la importancia de cada una de estas áreas de responsabilidad respecto de tu organización? Se trata de una reflexión clave y reveladora que te dará una visión general, siempre en función de la naturaleza de tu organización.

Responsabilidad	
Administración de identidades	**Liderada y soportada principalmente por la organización**
Autenticación & Autorización	
Gobierno y protección del dato	
Gobierno, cumplimento y legal	
Business continuity / Disaster recovery	
Seguridad física	
Cultura, concienciación y Conocimiento	
Descubrimiento y Gestión de Inventario	**Varía según el naturaleza de la organización**
Aplicaciones y Endpoints	
Administración de Dispositivos & Hosts	
Seguridad IT	**Delegada en proveedores especializados / Cloud / Otros**
Seguridad en Comunicaciones	
Seguridad en Almacenamiento	



Evaluando la madurez de tu organización

Una vez identificadas las áreas de responsabilidad, el siguiente paso es analizar las **competencias** vinculadas a las dichas áreas. Adelante, conoce a tu organización.

Área de responsabilidad	Competencia	Desarrollada [S N/ N/A]	Madurez [0-10] *
Administración de identidades	Administración centralizada de identidades		
Autenticación & autorización	Autenticación federada Saas & LOBs		
	SSO		
	Doble factor de atutentación		
	Roles & Grupos		
	Políticas & privilegios		
	Auditoría y monitorización		
	B2B vs B2C		
	Gestión de Identidad Privilegiada (PIM)		
	Gestión de Accesos Privilegiados (PAM)		
	Gestión de Identidades y Accesos (IAM)		
Gobierno y protección del dato	Categorización de la información		
	Protección del dato		
	Integridad del dato		
	Supervisión de correo, documentos y otros activos		
	Administración de claves, secretos y certificados		
Gobierno, cumplimento y legal	Categorización de la información		
	Definición de áreas de responsabilidad y asignación de competencias		
	Existencia de un Plan director de Seguridad		
	Instrucciones, directivas, procedimientos y estándares documentados		
	Estandares y Regulaciones (ISO 27001 ,SOX, HIPPA, PCI-DSS, GDPR)		
Business continuity / Disaster recovery	Existencia de un Plan de recuperación ante desastres		
	Simulacros periódicos controlados		
Seguridad física	Protección del puesto de trabajo		
	Controles de acceso		
	Gestión de autorizaciones		
Cultura y conocimiento	Formación		
	Evangelización		
	Conocimiento especializado		

* 0 Inmaduro - 10 Muy maduro

Evaluando la madurez de tu organización

Área de responsabilidad	Competencia	Desarrollada [S N/ N/A]	Madurez [0-10] *
Descubrimiento y gestión del inventario	Descubrimiento y gestión del inventario		
Aplicaciones y endpoints	Saas & LOBs		
	Integraciones		
	Client Endpoints		
	Desarrollos internos		
	Web app scaninng		
	Auditorías periódicas (Test intrusión, Pentesting, Spear Phising, Black/White Box)		
Administración de dispositivos y Hosts	Bring Your Own Device		
	Gestión de dispositivos móviles (MDM)		
	Gestión de aplicaciones móviles (MAM)		
	Administración de movilidad empresarial (EMM)		
Seguridad IT	Datacenter		
	Cloud Vendors		
	SIEM, SOC, VMDR		
	Actualización y parches de seguridad		
	Firewall		
	WAF		
	Load Balancing		
	ACLs		
	DooS Protection		
	Seguridad en MVs		
	Auditoría automática y periódica de vulnerabilidades		
	Administración y resolución de vulnerabilidades		
	Monitorización & alarmado		

* 0 Inmaduro - 10 Muy maduro

Evaluando la madurez de tu organización

Área de responsabilidad	Competencia	Desarrollada [S N/ N/A]	Madurez [0-10] *
Seguridad en comunicaciones	SSL/TLS		
	Certificados		
	Cifrado en tránsito		
	Cifrado en VPN		
	Network supervisor		
	Applications insights		
	Wifi		
Seguridad en almacenamiento	Cifrado de datos en reposo		
	Cifrado en tránsito		
	Cifrado en cliente		
	Cifrado en servidor		
	Cifrado en datastores		
	Cifrados de base de datos		

* 0 Inmaduro - 10 Muy maduro

¿Preocupado por el resultado? En absoluto, se trata de un reto continuado en el que Qualoom te puede ayudar.

Responsabilidad	SaaS	PaaS	IaaS	On-Prem	
Administración de identidades	✓	✓	✓	✓	Liderada y soportada principalmente por la organización
Autenticación & Autorización	✓	✓	✓	✓	
Gobierno y protección del dato	■	■	■	■	
Gobierno y cumplimento legal	■	■	■	■	
Business continuity / Disaster recovery	✓	✓	✓	✓	
Seguridad física	■	■	■	■	
Cultura y Conocimiento	✓	✓	✓	✓	
Descubrimiento y Gestión de Inventario	✓	✓	✓	✓	Varía según el naturaleza de la organización
Aplicaciones y Endpoints	▱	◪	■	■	
Administración de Dispositivos & Hosts	✓	✓	✓	✓	
Seguridad IT	✓	✓	✓	✓	Delegada en proveedores especializados / Cloud / Otros
Seguridad en Comunicaciones	✓	✓	✓	✓	
Seguridad en Almacenamiento	✓	✓	✓	✓	

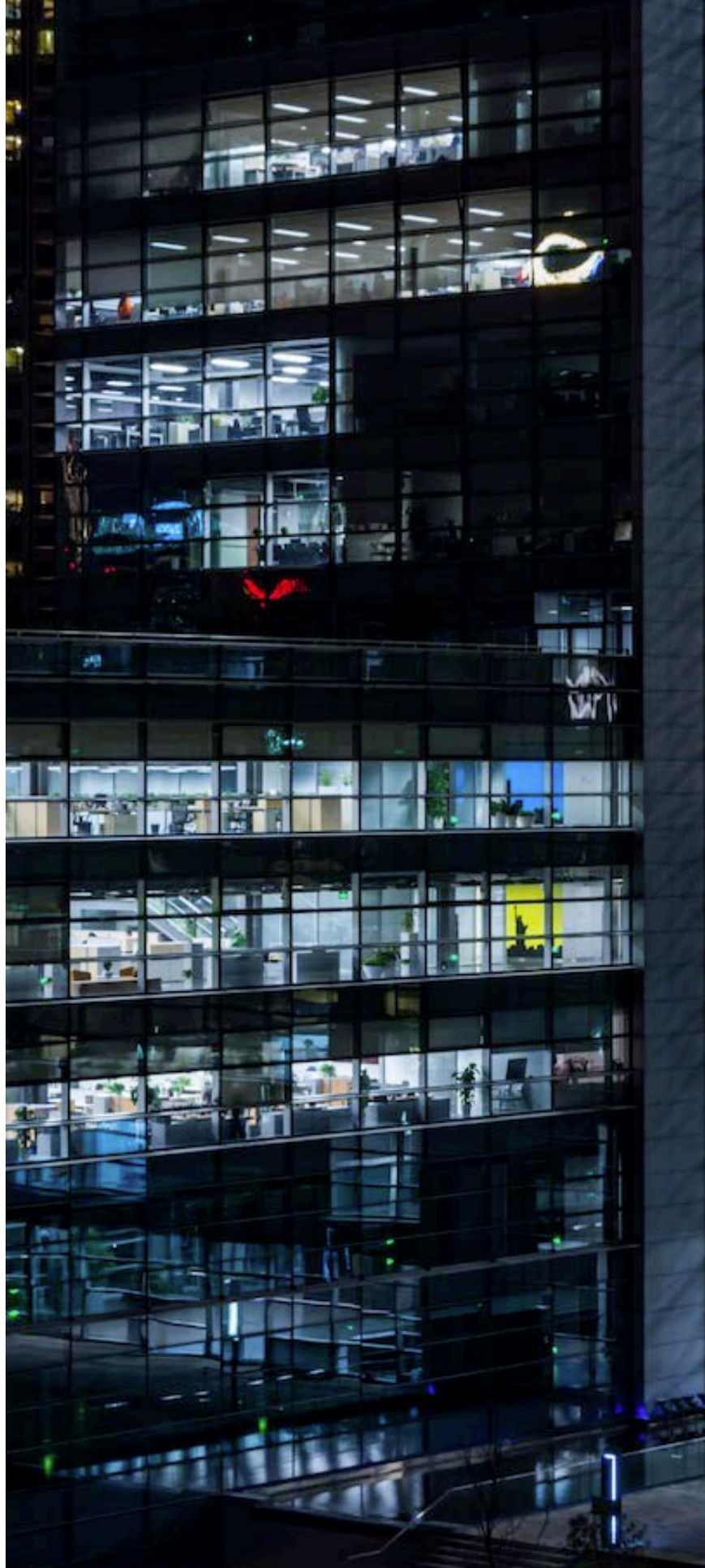
Y entonces ¿por dónde empiezo?

Sencillo. Demos un paso más. **Diagnóstico PoC.** Comienza analizando tu situación actual real durante una semana.

Para ello puedes hacerlo a través de este proyecto, pero es importante que respondas a esta pregunta. **¿Estás dispuesto a asumir que una vez finalizado van a aparecer vulnerabilidades y deficiencias? La seguridad 100% no existe.**

Pero en qué consiste:

- Coste simbólico del **Diagnóstico PoC** de 350 euros + IVA
- Desplegaremos una sondas para el descubrimiento de tus activos TI o seleccionaremos los que más te preocupen. No afectan a servicios ni comunicaciones, son meros observadores de todo lo que acontece y su configuración.
- Durante 1 semana de análisis se obtendrá una información de gran valor.
- Al finalizar el PoC te entregaremos un informe con el estado de tus organización o de los activos seleccionados, junto con una priorización de todas las vulnerabilidades, deficiencias y recomendaciones para que puedas proceder a su resolución.
- ¿Cómo? No tienes equipo para su resolución. No te preocupes, nosotros lo hacemos por ti o te ayudamos en el proceso a través de nuestro **Proyecto DevSecOps.**



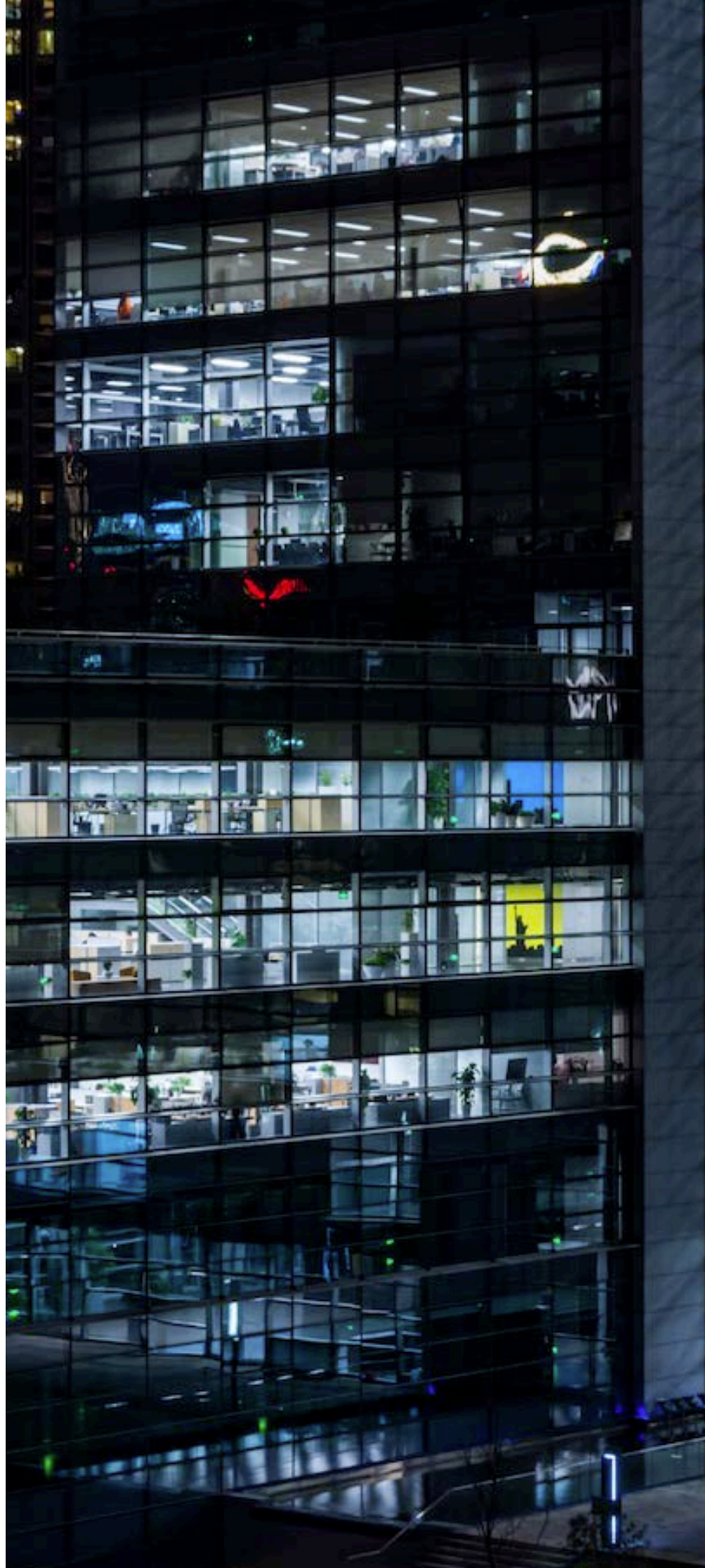
Proyecto DevSecOps

Se trata de un proyecto de consultoría de Seguridad 360 que ofrecemos a organizaciones de cualquier tamaño, consistente en:

- Monitorización continuada de tus activos
- Categorización y priorización de vulnerabilidades detectadas.
- Soporte a la resolución de dichas vulnerabilidades.
- Informes de cumplimiento automáticos y supervisado por personal cualificado

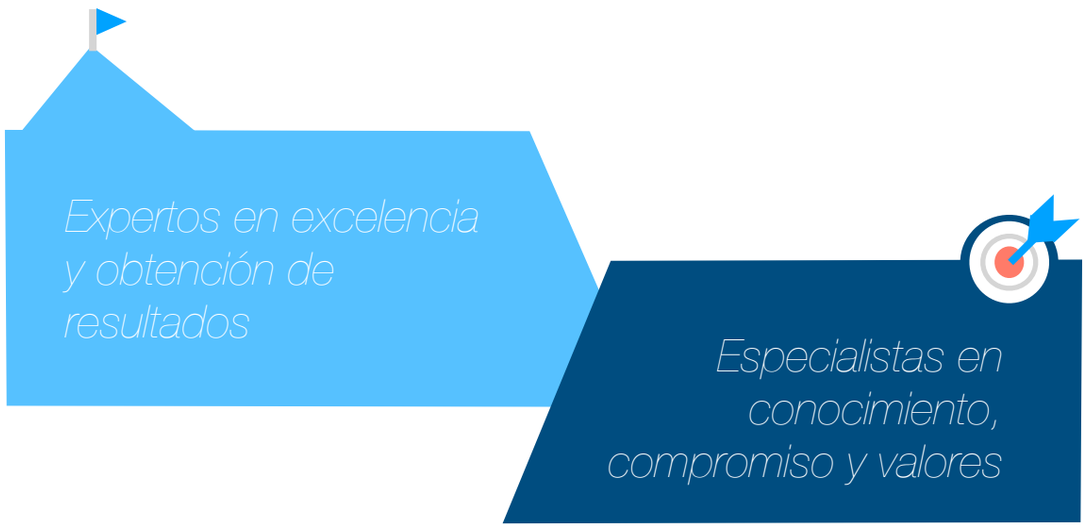
¿Coste?

Entry	Medium	Extended
1 jornada / mes resolución	1,5 jornada / mes resolución	2 jornada / mes resolución
100 activos	200 activos	300 activos
930 € / mes	**1.500 € / mes**	**2.000 € / mes**



Y ahora un poco sobre nosotros

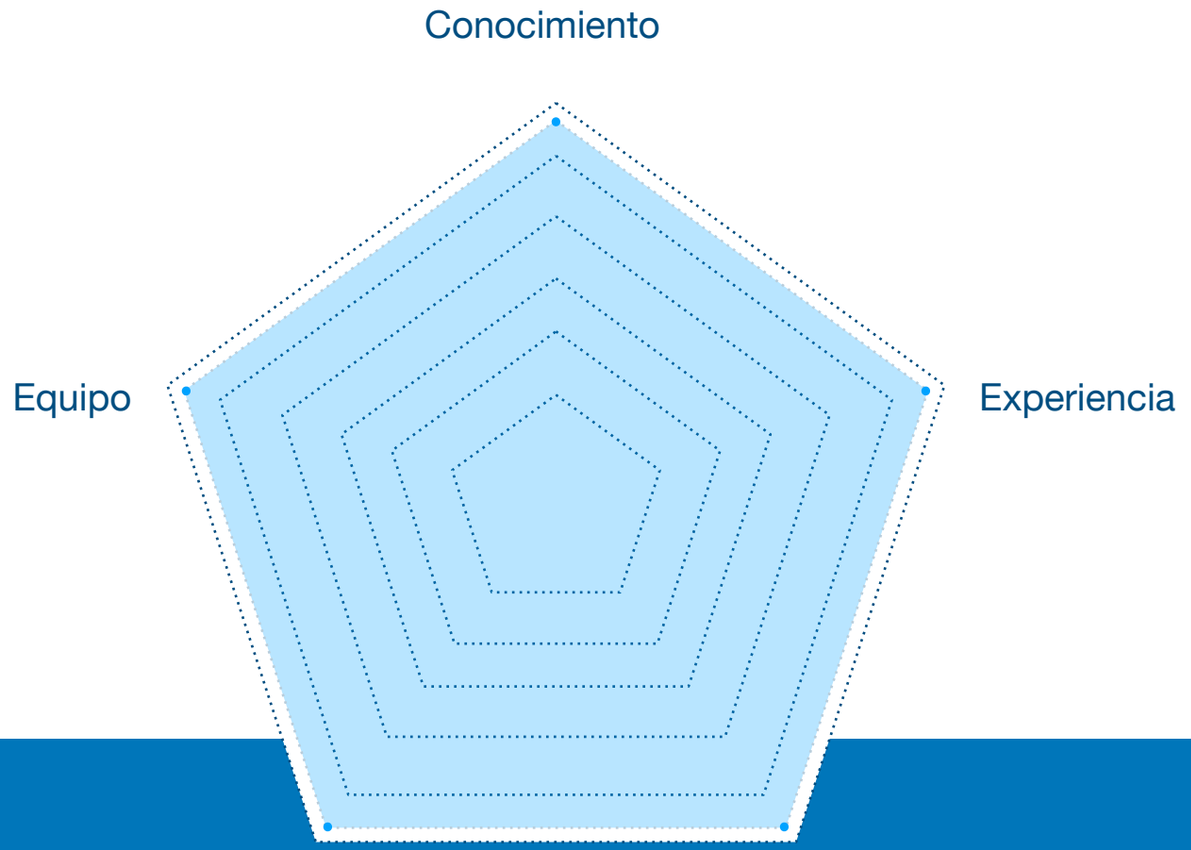
Qualoom Expertise Technology es una compañía española del sector de las tecnologías de la información con más de 12 años de experiencia, que desarrolla su actividad en el ámbito de la Consultoría IT, Cloud, Infraestructura, Alto rendimiento, Escalabilidad, optimización de Costes, DevOps/DevSecOps y Seguridad que cuenta con un equipo de especialistas y una red de Partners que nos permiten abordar proyectos críticos para cualquier organización.



POR QUÉ NOSOTROS
POR QUÉ QUALOOM

Ofrecemos soluciones tecnológicas reales alineadas con las necesidades de nuestros clientes convirtiéndonos en parte del equipo y en su **socio tecnológico.**

Todas nuestras actuaciones se basan en una plena relación de confianza tecnológica para el correcto desarrollo de la estrategia de negocio y su respaldo tecnológico.



La percepción del valor es la mejor garantía de un trabajo bien realizado.

Director de Sistemas

Qualoom Expertise Technology

NUESTRO SECRETO
EL EQUIPO

Nuestro secreto es nuestro equipo. Un conjunto de profesionales especializados en las áreas más críticas de la innovación al servicio del día a día de las organizaciones más exigentes.

Contamos con **certificaciones** en los ámbitos más importantes como son la Gestión de Procesos TI, Infraestructuras y Servicios Cloud.

aws partner network

Advanced
Consulting
Partner

Digital Customer Experience Competency

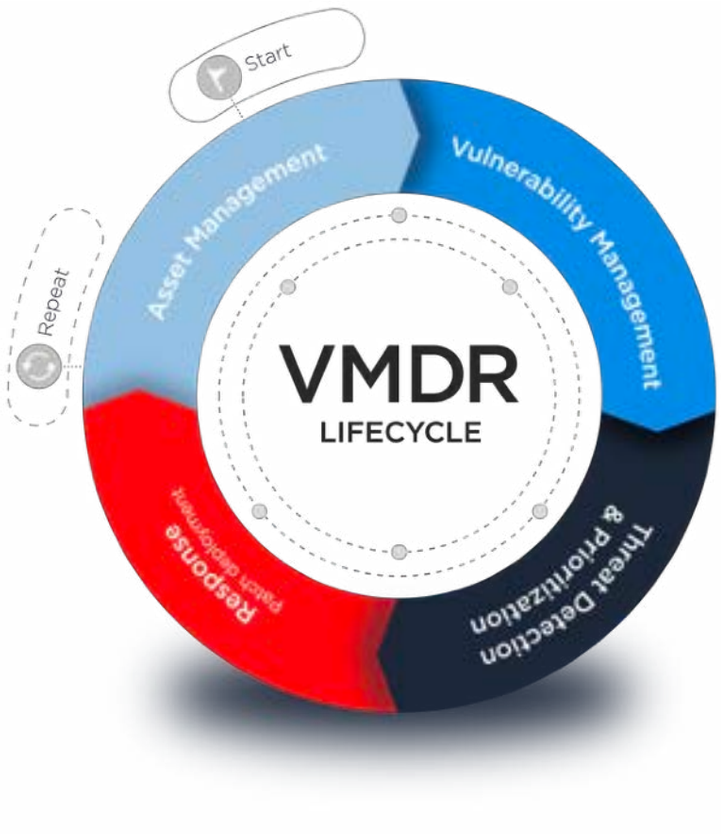
Solution Provider

Google Cloud
Partner

Microsoft
Silver Partner

Qualys Partner

VMDR



En materia de seguridad, Qualoom es **Partner de Qualys desde 2020** y especialista en la implementación de su plataforma VMDR y otros servicios/apps satélites que permite descubrir, evaluar, priorizar y resolver vulnerabilidades críticas en tiempo real, de manera global a la organización, de forma sostenida en el tiempo y con independencia de la tipología de activos y entornos existentes.

www.qualys.es

Robota Partner

robota VAP

Además, Qualoom es **Partner de Robota** a través de su plataforma VAP que permite descubrir, evaluar, priorizar y resolver vulnerabilidades críticas en tiempo real y de manera global a la organización, con independencia de a tipología de activos y entorno existente.

Adicionalmente el equipo de ingenieros de seguridad de Robota y de Qualoom ofrece un servicio de acompañamiento en todo el proceso de implantación de la solución, análisis, detección y resolución de amenazas.

https://www.robota.net/

Amazon Web Services Partner

Qualoom Expertise forma parte de la red de socios de Amazon Web Service como **Partner Advance** con más de 10 años de experiencia en proyectos críticos de migraciones, DevOps, Seguridad, rendimiento, optimización de costes y alta escalabilidad.

En materia de seguridad estos son los servicios más importantes para el gobierno y gestión de la seguridad dentro de este ecosistema.

Amazon Web Services
Partner · Seguridad de la información

Identity & Access Management	Administre de manera segura el acceso a los servicios y los recursos	**AWS Identity & Access Management (IAM)**
	Servicio de inicio de sesión único (SSO) en la nube	**AWS Single Sign-On**
	Administración de identidades para las aplicaciones	**Amazon Cognito**
	Microsoft Active Directory administrado	**AWS Directory Service**
	Servicio simple y seguro para compartir recursos de AWS	**AWS Resource Access Manager**
	Gobernanza y administración centralizadas en cuentas de AWS	**AWS Organizations**
Detección	Centro unificado de seguridad y conformidad	**AWS Security Hub**
	Servicio administrado de detección de amenazas	**Amazon GuardDuty**
	Analice la seguridad de las aplicaciones	**Amazon Inspector**
	Registre y evalúe las configuraciones de sus recursos de AWS	**AWS Config**
	Realice un seguimiento de la actividad de los usuarios y el uso de las API	**AWS CloudTrail**
	Administración de la seguridad para dispositivos compatibles con IoT	**AWS IoT Device Defender**
Respuesta frente a incidencias	Investigue los posibles problemas de seguridad	**Amazon Detective**
	Recuperación ante desastres rápida, automatizada y rentable	**CloudEndure Disaster Recovery**

Amazon Web Services
Partner

Protección de infraestructuras	Seguridad de la red	**AWS Network Firewall**
	Protección frente a ataques DDoS	**AWS Shield**
	Filtre el tráfico web malintencionado	**AWS Web Application Firewall (WAF)**
	Administración central de reglas de Firewall	**AWS Firewall Manager**
Protección de datos	Descubra y proteja sus datos confidenciales a escala	**Amazon Macie**
	Administración y almacenamiento clave	**AWS Key Management Service (KMS)**
	Almacenamiento de claves en hardware a efectos de conformidad normativa	**AWS CloudHSM**
	Aprovisionamiento, administración e implementación de certificados públicos y privados SSL/TLS	**AWS Certificate Manager**
	Alterne, administre y recupere datos confidenciales	**AWS Secrets Manager**
Conformidad	Portal gratuito autoservicio para el acceso bajo demanda a los informes de conformidad de AWS	**AWS Artifact**
	Realice auditorías del uso de AWS de forma continua para simplificar la forma en que evalúa el riesgo y la conformidad	**AWS Audit Manager**

NUESTRA CARTA DE PRESENTACIÓN
CASOS DE ÉXITO

A continuación presentamos otros referencias y y casos de confianza en nuestro equipo Disponemos de **excelentes referencias** sobre nuestros servicios, por lo que no dude en solicitarlas si lo considera de interés.

vocento

Telefónica

hm hospitales

TUI

Interflora

TiendAnimal

LaLiga

ENGIE

TECHNOACTIVITY

danosa

Viena Capellanes

TWIN PUSH

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

MYMOID

MELIÃ HOTELS INTERNATIONAL

ma·mu·ky FOR KIDS

REAL INSTITUTO elcano 20 ROYAL INSTITUTE AÑOS·YEARS

BRICO DEPÔT

KRACK

federópticos

CONTACTO
SIEMPRE DISPONIBLES

Qualoom Expertise Technology S.L
Plaza de Valencia 6
Móstoles, Madrid 28937

Teléfono: +34 91 236 48 08
E-mail: info@qualoom.es
Web: http://www.qualoom.es