EXTENDED DETECTION & RESPONSE

# Cloud Security

¿CÓMO TE AYUDAMOS DESDE TELEFÓNICA TECH?

## Migra a la nube con confianza con una solución de seguridad diseñada para proteger los activos y aplicaciones de tu empresa en todo su ciclo de vida

La transformación digital de las empresas está íntimamente ligada a la adopción de la nube pública, que introduce un nuevo paradigma de responsabilidad compartida con los proveedores (CSPs) y nuevos retos de seguridad.

Según Gartner, el 95% de los problemas de seguridad en la nube son generados por el propio cliente.
El cambio radical en la provisión de servicios basado en interfaces programáticas, la falta de visibilidad de las cargas de trabajo subidas a la nube o las metodologías Agile y prácticas DevOps asociadas a la cloud, donde la seguridad suele pasar a un segundo plano, hacen que sea bastante fácil exponer la infraestructura en la nube por problemas de seguridad como los errores de configuración.

Cloud Security de Telefónica Tech es una solución de seguridad diseñada para identificar, evaluar y gestionar todos los retos y amenazas de la nube de forma integral. Las compañías necesitan proteger las cargas de trabajo en todo su ciclo de vida, desde las fases de codificación y CI/CD a la fase de ejecución, cuando son desplegadas en la nube. Aparece el concepto "shift-left security" que permite a las organizaciones construir aplicaciones de manera segura sin perder agilidad.

¿A QUIÉN VA DIRIGIDO ESTE SERVICIO?

Organizaciones en nube pública (AWS, Azure, GCP, OCI, Alicloud) o nube híbrida, preocupadas por la falta de visibilidad, control y gobierno en la nube y en los procesos DevOps.

Clientes que quieren un servicio recurrente que implemente un assessment continuo de la seguridad en la cloud.

Organizaciones que tengan un volumen relevante de activos en nube pública y/o privada en sus modalidades IaaS y PaaS.

NUESTRA PROPUESTA DE VALOR

## Nuestro servicio

El servicio de Seguridad en Cloud Gestionada, Cloud Security, de Telefónica Tech tiene como objetivo devolver el control de la seguridad en la nube pública e híbrida a los CISOs y responsables de seguridad por medio de unas capacidades que permiten proteger los activos y aplicaciones en todo su ciclo de vida.

El servicio está basado en tecnologías nativas de seguridad cloud como CNAPP (Cloud Native Application Protection Platform). Por encima de la tecnología, el servicio ofrece un conjunto de procesos y entregables que van a permitir a nuestros clientes tener una visión de alto nivel de la seguridad en la nube basada en KPIs y ver su evolución basada en la mejora continua.

## ¿Qué te permite?

El servicio te permitirá tener las siguientes capacidades:

› **Capacidad Posture Governance:** para visibilidad y gobierno de los activos desplegados en cloud, con esta capacidad se realiza un assessment continuo de seguridad conforme a un marco de políticas adaptado al contexto el cliente.

› **Capacidad Monitoring:** protección runtime de los workloads que ejecutan las aplicaciones. Detección de actividad sospechosa como Malware & cryptomining o comunicación con IPs de mala reputación. Un 24x7 de triaje y tratamiento de alertas.

› **Capacidad Shift-left:** bastionado de los workloads, se realiza un escaneo de vulnerabilidades y buenas prácticas en los workloads de cómputo desplegados en la nube.

› **Capacidad Workload Super-Vision:** con esta capacidad se mueven los controles de seguridad a la izquierda: a las fases de desarrollo y CI/CD. Se incluye el escaneo de registros de contenedores, repositorios de código o el CI, entre otras funcionalidades.

## Beneficios del servcio

### Dinámica de entregables

Nuestro servicio entrega de forma periódica reportes con incumplimientos y vulnerabilidades de la infraestructura cloud y aplicaciones en todo su ciclo de vida. Estos reportes están acompañados de un plan de acción para solventar los incumplimientos más relevantes. Adicionalmente, se incluyen indicadores de alto nivel que van a permitir ver el estado de la seguridad, su evolución y ayudar a determinar el plan de acción, de cara a mejorar de forma continua la seguridad y promover un cambio cultural en la compañía.

### El servicio es más que una herramienta de seguridad.

Olvídate de gestionar complejas plataformas de seguridad en la nube. El servicio ofrece una visión de alto nivel basada en KPIs que permite supervisar la seguridad en la nube y ver la evolución basada en la mejora continua.

### Monitorización 24x7

Para las alertas de seguridad que requieren un tratamiento proactivo se incluye un 24x7 donde se hará un triaje de las alertas, descartando falsos positivos e incluyendo recomendaciones de cara a la remediación, en caso de que la amenaza se confirme.

## Valor diferencial de Telefónica Tech

Nuestro equipo se encarga de la entrega y configuración de la plataforma CNAPP, utilizada por el servicio, proporcionando una estrecha orientación y apoyo durante todo el proceso de despliegue y operación.

Nuestro equipo de Cloud Security está enfocado en la seguridad en la nube e integrado en el iSOC.

Cloud Security es un servicio personalizado que se adapta al contexto del cliente, tanto en configuración de controles y políticas como es las acciones de remediación.

EQUIPO Y LOGROS

### Nuestros equipos

- **1.800** empleados de SecOps.
- **+1.500** certificaciones de seguridad.
- **+30** analistas de Cloud MSS.

### Logros

- Un amplio espectro de referencias nos convierte en **uno de los principales MSSP en la nube.**
- Entre nuestros principales clientes están incluidas varias **compañías del Ibex 35.**
- **Partner Cloud MSSP certificado** por los principales fabricantes de seguridad cloud.

MODELO COMERCIAL

Es un servicio que ofrece una **suscripción anual** que tiene todo lo necesario para dotar de seguridad tanto la nube pública y privada como los procesos DevOps.

La cotización está basada en el número de cargas de trabajo o activos protegidos. El servicio tiene tres modalidades que incluyen las diferentes capacidades del servicio:

- Modalidad **Governance**: incluye la capacidad Posture Governance.
- Modalidad **Defense**: incluye las capacidades de Monitoring, Workload Super-Vision y Shift-left Security.
- Modalidad **Advanced:** une las capacidades de Cloud MSS Governance y Cloud MSS Defense.

PARTNERS RELACCIONADOS

paloalto NETWORKS

SERIVICIOS RELACCIONADOS

### SIEM Management

Monitorización y correlación de eventos de seguridad con gestión de alertas e incidentes en 24x7, proporcionando una base sólida en la detección de amenazas de seguridad.

Contáctanos para empezar la transformación digital de tu organización.