

# Seguridad en la nube

## Consultoría en capacidades de Ciberseguridad

### Descripción del Servicio

El servicio de Seguridad en la Nube está orientado a proteger infraestructuras cloud, prevenir y mitigar incidentes de seguridad y definir estrategias de recuperación. Las soluciones cloud permiten aprovisionar recursos bajo demanda y de forma escalable, pero operan bajo un modelo de responsabilidad compartida entre proveedor cloud y organización, por lo que se requiere una estrategia de seguridad adecuada para garantizar el funcionamiento y cumplimiento normativo.

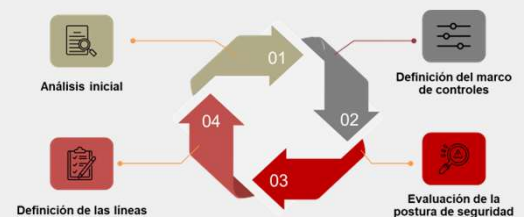
Las áreas clave en las que se enfoca el servicio incluyen la gestión de las configuraciones y vulnerabilidades, monitorización y detección de incidentes, protección de la información y seguridad de red, así como gestión y seguridad de puntos de acceso e identidades (IAM). La seguridad cloud mejora la confianza y reputación, aumenta la disponibilidad y continuidad de los servicios, protege los datos y facilita el cumplimiento normativo, reduciendo costes por posibles sanciones y pérdidas financieras.

Entre los retos destacan la gestión del ciclo de vida de los datos, la unificación y gobernanza de configuraciones, la protección de identidades como principal vector de ataque, el cumplimiento de normativas y la falta de visibilidad y control. Una gestión deficiente puede facilitar el robo de información, exposiciones por configuraciones inseguras y accesos no autorizados, convirtiendo a las infraestructuras cloud en objetivos atractivos para actores maliciosos.

### Tipos de Servicio

#### Revisión de la postura de seguridad y auditorías de seguridad

Servicio para **evaluar el estado de seguridad cloud** mediante un análisis inicial y la evaluación de los entornos en base a un marco de controles, identificando brechas y priorizando acciones de mejora. Este servicio ayuda a **mejorar la visibilidad** de la organización y **definir planes de acción** para mejorar la postura; sin ella se mantienen riesgos no detectados y decisiones de seguridad poco fundamentadas.



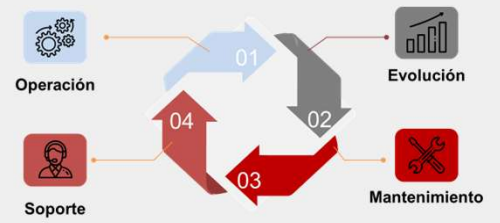
#### Implantación de soluciones o herramientas de seguridad

Servicio de **selección, definición e implantación de herramientas de seguridad** (SIEM, EDR, XDR, etc.) según necesidades, con despliegue e integración controlada y ajustes y fine-tuning posteriores. **Mejora las capacidades** defensivas y la detección/protección; una implantación inadecuada puede generar mal rendimiento, **brechas de seguridad** o interferencias con el resto del ecosistema cloud de la organización.



## Gestión, mantenimiento y evolución de soluciones de seguridad

Servicio continuo de **operación, soporte, mantenimiento y evolución** funcional de las herramientas de seguridad de la organización para mantenerlas **efectivas y alineadas** con posibles nuevos requisitos. Garantiza la **disponibilidad y adaptación** de la herramienta; su ausencia degrada la eficacia de las soluciones y **aumenta la exposición a incidentes**.



## Definición de estrategias de Backup y Disaster Recovery (DS)

Servicio que busca diseñar e implementar la **infraestructura y procesos de backup** y recuperación (RTO/RPO, planes y pruebas) para asegurar la **continuidad de servicios críticos**. Reduce impacto y riesgos en incidentes graves; sin una estrategia adecuada se corre el riesgo de pérdida irreversible de datos y paralización de servicios.



## Soporte en la migración de los sistemas on-premise a entornos cloud

Servicio de asesoría y ejecución **para migrar sistemas a la nube de forma segura** (inventario, arquitectura objetivo, pilotaje, migración por oleadas y validación). **Minimiza errores** de configuración y vulnerabilidades derivadas de la migración; sin soporte aumentan las probabilidades de **fallos operativos y brechas de seguridad**.



## Certificaciones necesarias



### SC-100: Microsoft Cybersecurity Architect

Valida la experiencia en la implementación y mantenimiento de soluciones de seguridad de Microsoft Azure.



### AWS Certified Security - Specialty

Valida la experiencia en la creación y mantenimiento de soluciones de seguridad en AWS.



### CCSP – Certified Cloud Security Professional

Valida conocimientos avanzados en el diseño gestión y seguridad de aplicaciones e infraestructura Cloud (+5 años de experiencia).



### Certificate of Cloud Security Knowledge (CCSK)

Valida conocimientos en todos los ámbitos de la seguridad cloud de entornos multi-nube.



### ISO/IEC 22301

Estándar internacional que establece los requisitos para establecer y mantener un Sistema de Gestión de la Continuidad del Negocio (SGCN).



### ISO/IEC 27001

Estándar internacional que establece los requisitos para establecer y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).

## Valor comercial del servicio

Los datos muestran que la seguridad en la nube es clave para el ecosistema navarro: el aumento de la inversión global en seguridad cloud y la proliferación de aplicaciones SaaS impulsan la adopción de la nube, lo que mejora la digitalización y la eficiencia organizativa pero también aumenta los riesgos si no se protege adecuadamente.

Muchas organizaciones en Navarra carecen de la experiencia necesaria para asegurar sus entornos cloud, lo que crea vulnerabilidades especialmente en el tejido industrial altamente digitalizado y en las PYMES, que suponen una oportunidad de mercado para servicios de seguridad en la nube; además, sectores ya digitalizados como Farma/Salud, Agroalimentario, TIC y Energía presentan potenciales áreas de mejora en relación a la seguridad en la nube.

