qualoom®

Inspiring Technology
for People

Manual de seguridad para entornos cloud native (políticas, controles, IAM)

Área de Cloud e Infraestructura
Fecha 09/07/2026
Versión 1.0
Clasificación: Público

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

ÍNDICE

qualoom®

Inspiring Technology
for People

Introducción: Seguridad en Entornos Cloud-Native

La adopción de arquitecturas **cloud-native** ha transformado radicalmente la forma en que las organizaciones diseñan, despliegan y operan sus plataformas tecnológicas. Modelos basados en **microservicios, contenedores, orquestadores y servicios serverless** permiten alcanzar altos niveles de escalabilidad, resiliencia y eficiencia operativa. Sin embargo, este cambio de paradigma introduce nuevos desafíos en materia de **seguridad, gobernanza y control.**

A diferencia de los entornos tradicionales on-premise, donde los perímetros eran claramente definidos, los ecosistemas cloud-native operan bajo un modelo **dinámico, distribuido y altamente automatizado,** donde los recursos son efímeros, las identidades reemplazan al perímetro y la infraestructura se define como código.

En este contexto, la seguridad deja de ser un componente reactivo y pasa a convertirse en un **habilitador estratégico del negocio,** integrada desde el diseño inicial de la arquitectura hasta la operación continua de los servicios.

qualoom®

Inspiring Technology
for People

Principios de Seguridad en Entornos Cloud-Native

La seguridad en entornos cloud-native debe basarse en una serie de principios fundamentales que garanticen consistencia, escalabilidad y resiliencia frente a amenazas modernas.

Seguridad como Código (Security as Code)

La seguridad debe ser tratada como un artefacto más del ciclo de vida del software. Esto implica:

- Definir políticas, configuraciones y controles mediante **IaC.**
- **Versionar y auditar** los cambios de seguridad.
- **Automatizar** validaciones y despliegues seguros.

Este enfoque **reduce errores humanos** y asegura coherencia entre entornos.

Principio de Menor Privilegio

Toda identidad (humana o de servicio) debe contar **únicamente con los permisos estrictamente necesarios** para realizar su función. Este principio minimiza el impacto de accesos indebidos, credenciales comprometidas o errores de configuración.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Principios de Seguridad en Entornos Cloud-Native

Defensa en Profundidad (Defense-in-Depth)

La seguridad no debe depender de un único control, sino de múltiples capas superpuestas, incluyendo:

- Controles de identidad
- Seguridad de red
- Protección de workloads
- Monitorización y detección
- Respuesta automatizada

Automatización y Escalabilidad Segura

Dado el carácter dinámico del cloud, los controles de seguridad deben escalar automáticamente y adaptarse a cambios constantes en la infraestructura, sin introducir fricción operativa.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Gestión de Identidades y Acceso (IAM)

La identidad es el nuevo perímetro en entornos cloud-native. Un modelo IAM mal diseñado representa uno de los mayores riesgos de seguridad.

Modelo de identidades y principio de mínimo privilegio

El modelo IAM debe estructurarse diferenciando claramente los tipos de identidad y su ámbito de actuación:

Identidades humanas

Autenticadas a través de proveedores de identidad corporativos y sujetas a controles reforzados.

Identidades técnicas

Asociadas a aplicaciones, microservicios y procesos automatizados, con permisos estrictamente limitados.

Roles

Como mecanismo principal de asignación de privilegios, preferentemente de carácter temporal y reutilizable.

Grupos y políticas

Utilizados para estandarizar permisos, facilitar la gobernanza y asegurar la trazabilidad.

La asignación de accesos debe basarse sistemáticamente en el principio de menor privilegio, evitando permisos persistentes o excesivos y reduciendo la superficie de ataque.

qualoom®

Inspiring Technology
for People

Gestión de Identidades y Acceso (IAM)

Autenticación, federación y control contextual

El modelo IAM debe estructurarse diferenciando claramente los tipos de identidad y su ámbito de actuación:

Autenticación multifactor (MFA)

Obligatoria para usuarios privilegiados y operaciones sensibles.

Federación de identidades

Con directorios corporativos, minimizando la gestión de identidades locales en la nube.

Evaluación contextual del acceso

Considerando factores como rol, ubicación, dispositivo y nivel de riesgo, en línea con un modelo Zero Trust.

La autorización debe implementarse mediante políticas granulares, desacoplando identidades de permisos directos.

Gestión segura de credenciales y secretos

La gestión de credenciales en entornos cloud-native debe ser centralizada y automatizada:

- Uso de servicios gestionados de secretos para claves, certificados y tokens.
- Rotación automática y periódica de credenciales.
- Eliminación de credenciales estáticas siempre que sea viable.
- Prohibición del almacenamiento de secretos en código, repositorios o imágenes de contenedores.

Este enfoque es fundamental para mitigar riesgos asociados a fugas de información y compromisos de identidad.

qualoom®

Inspiring Technology
for People

Gestión de Identidades y Acceso (IAM)

Gobernanza, auditoría y control continuo

El modelo IAM debe integrarse dentro de un marco de gobernanza y control continuo, que permita:

- Revisiones periódicas de roles y permisos para detectar desviaciones del modelo definido.
- Registro centralizado e inmutable de accesos y actividades.
- Monitorización de comportamientos anómalos y accesos no habituales.
- Generación de evidencias trazables para auditoría y cumplimiento normativo.

En entornos cloud-native, la gestión de identidades no debe considerarse un estado estático, sino un proceso continuo, alineado con la evolución de la arquitectura, los riesgos y los requisitos regulatorios.

qualoom®

Inspiring Technology
for People

Políticas de **Seguridad y Gobernanza**

La gobernanza de seguridad en entornos cloud-native garantiza que el uso de los recursos en la nube se mantenga **alineado con los objetivos corporativos, los requisitos regulatorios y el marco de riesgos**, mediante políticas estandarizadas y controles auditables.

Definición de políticas cloud-native

Las políticas de seguridad deben diseñarse específicamente para entornos cloud-native, priorizando la automatización, la escalabilidad y el control preventivo. Estas políticas deben cubrir, como mínimo, **los siguientes ámbitos:**

Gestión de identidades y accesos

definiendo criterios de asignación, uso de roles, autenticación reforzada y segregación de funciones.

Configuración segura de recursos

estableciendo estándares de hardening, restricciones de red y parámetros de seguridad por defecto.

Protección de datos

incluyendo clasificación de la información, cifrado en tránsito y en reposo, y control de accesos a datos sensibles.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Políticas de **Seguridad y Gobernanza**

Uso aceptable y segregación de entornos

garantizando la separación efectiva entre entornos de desarrollo, pruebas y producción.

Las políticas deben ser claras, medibles y directamente traducibles a controles técnicos.

Gobernanza y cumplimiento normativo

El marco de seguridad cloud debe alinearse con las principales normativas y estándares de referencia aplicables al negocio, tales como:

GDPR

en materia de protección de datos personales y privacidad.

ISO/IEC 27001

como marco de gestión de la seguridad de la información.

HIPAA

en entornos con información sanitaria.

SOC 2

para entornos orientados a servicios y terceros.

La gobernanza debe asegurar que los requisitos regulatorios se integren desde el diseño de la arquitectura, evitando enfoques reactivos o dependientes de controles manuales.

qualoom®

Inspiring Technology
for People

Políticas de **Seguridad y Gobernanza**

Gobernanza y cumplimiento normativo

Dado el carácter dinámico de la nube, el cumplimiento normativo no puede basarse en evaluaciones puntuales. El uso de herramientas de Cloud Security Posture Management (CSPM) y escaneo de Infraestructura como Código (IaC) permite:

- Detectar automáticamente desviaciones respecto a las políticas definidas.
- Aplicar controles preventivos antes del despliegue de recursos.
- Generar evidencias consistentes y trazables para auditoría.
- Reducir la dependencia de revisiones manuales.

Este enfoque favorece un modelo de **cumplimiento continuo,** alineado con prácticas DevSecOps.

Gobernanza y cumplimiento normativo

Las políticas de seguridad deben gestionarse como activos vivos, siguiendo un ciclo de mejora continua que incluya:

Definición → **Implementación** → **Monitorización** → **Revisión y mejora continua**

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Controles de infraestructura y configuración

La infraestructura en entornos cloud-native debe diseñarse y desplegarse bajo el principio de secure-by-default, de forma que todos los recursos incorporen controles de seguridad desde su creación.

Seguridad de red

La seguridad de red constituye una de las primeras capas de protección de la infraestructura cloud y debe basarse en una **segmentación lógica estricta:**

- **Segmentación mediante VPC/VNET y subredes,** separando cargas de trabajo según su criticidad y función.
- **Uso de firewalls, Network Security Groups (NSGs) y security groups** para controlar el tráfico entrante y saliente.
- **Restricción del tráfico mediante listas blancas**, permitiendo únicamente las comunicaciones necesarias.
- **Inspección y control del tráfico este-oeste**, limitando la propagación lateral de amenazas dentro del entorno.

Este enfoque **reduce el impacto de posibles compromisos y mejora la trazabilidad de las comunicaciones.**

qualoom®

Inspiring Technology
for People

Controles de infra y configuración

Hardening de recursos y configuración segura

Todos los recursos cloud deben desplegarse siguiendo estándares de configuración segura previamente definidos:

- **Hardening de instancias y servicios gestionados,** eliminando servicios innecesarios y aplicando configuraciones mínimas.
- **Cifrado de datos en tránsito y en reposo,** utilizando mecanismos nativos del proveedor cloud.
- **Eliminación de configuraciones por defecto inseguras,** sustituyéndolas por plantillas aprobadas y versionadas.

La estandarización de configuraciones permite reducir errores humanos y garantizar coherencia entre entornos.

Protección de workloads

Todos los recursos cloud deben desplegarse siguiendo estándares de configuración segura previamente definidos:

- **Seguridad de endpoints,** mediante agentes o servicios gestionados de protección.
- **Control de acceso a APIs,** limitando su exposición y autenticando todas las llamadas.
- **Escaneo continuo de configuraciones y vulnerabilidades,** tanto en tiempo de despliegue como en operación.

Estos controles permiten detectar desviaciones de seguridad de forma temprana y mantener un nivel de protección consistente.

qualoom®

Inspiring Technology
for People

Seguridad en **contenedores y Orquestadores**

El uso de contenedores y orquestadores introduce **nuevas superficies de ataque asociadas a la compartición de recursos y la automatización,** por lo que la seguridad debe abordarse de forma integral desde las imágenes hasta la operación del orquestador.

Seguridad de imágenes de contenedores

Uso exclusivo de **imágenes confiables, verificadas y firmadas,** procedentes de repositorios controlados.

Escaneo automático de vulnerabilidades durante las fases de build y despliegue.

Eliminación de dependencias innecesarias, reduciendo la superficie de ataque y el tamaño de las imágenes.

Seguridad en orquestadores (Kubernetes)

Los orquestadores deben configurarse siguiendo principios de mínimo privilegio y aislamiento:

Implementación de RBAC estricto, limitando los permisos de usuarios y servicios.

Definición de Network Policies para controlar el tráfico entre pods y namespaces.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Seguridad en **contenedores y Orquestadores**

Gestión segura de secretos, evitando su exposición en manifiestos o imágenes.

Aislamiento de namespaces y workloads, separando cargas según criticidad y función.

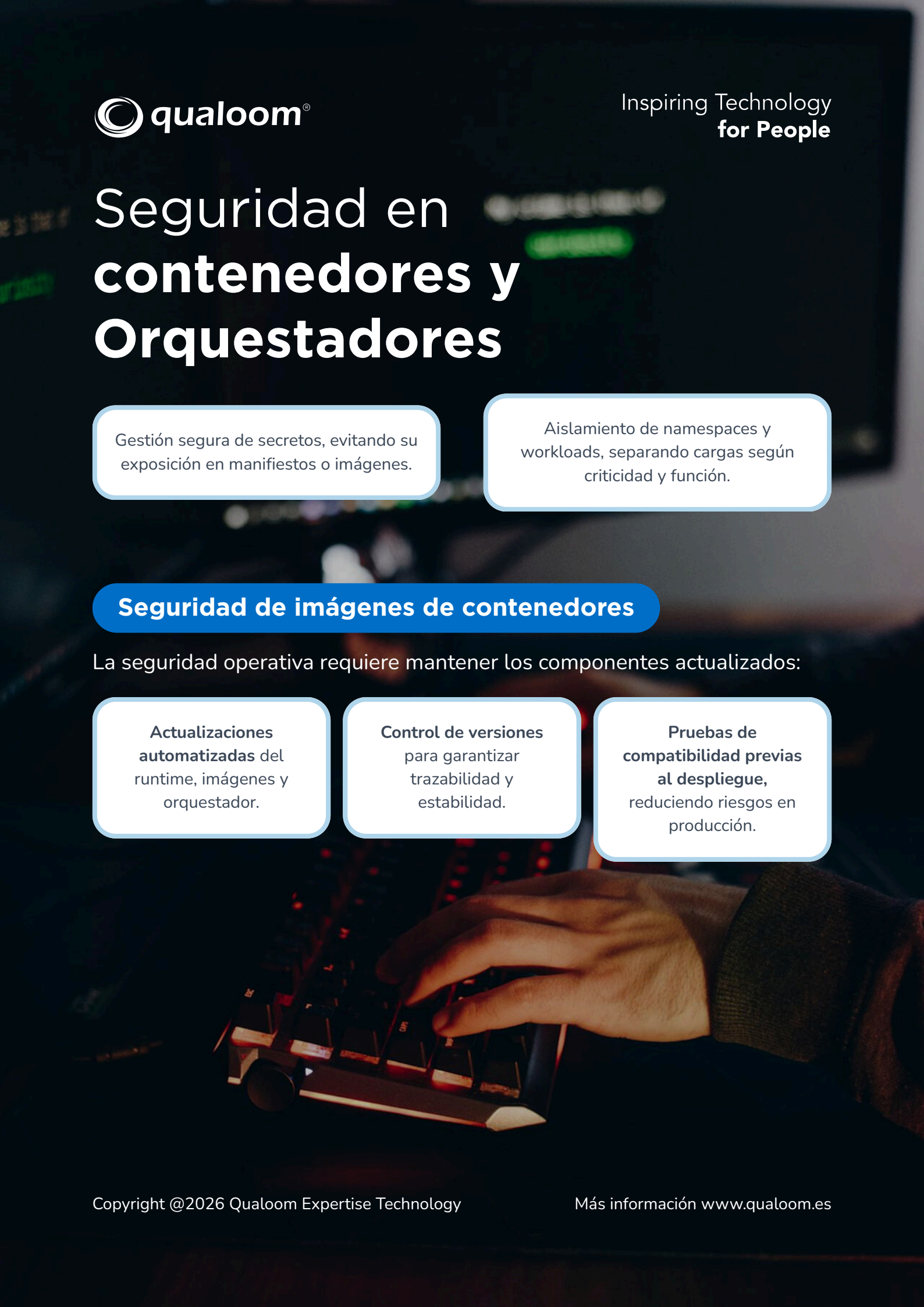
Seguridad de imágenes de contenedores

La seguridad operativa requiere mantener los componentes actualizados:

Actualizaciones automatizadas del runtime, imágenes y orquestador.

Control de versiones para garantizar trazabilidad y estabilidad.

Pruebas de compatibilidad previas al despliegue, reduciendo riesgos en producción.



Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Monitorización, auditoría y respuesta a incidentes

En entornos cloud-native, la visibilidad continua es fundamental para detectar, analizar y mitigar amenazas antes de que impacten la operación. La seguridad efectiva requiere integrar monitorización, auditoría y respuesta en un flujo continuo y automatizado.

Monitorización centralizada

La monitorización debe consolidar información de toda la infraestructura y aplicaciones

01

Recolección de logs, métricas y eventos

Agrupación de datos de infraestructura, contenedores y aplicaciones para obtener un panorama completo de la actividad del entorno cloud.

02

Correlación de eventos de seguridad

Análisis de patrones y relaciones entre eventos para identificar incidentes complejos que no serían visibles de forma aislada.

03

Alertas basadas en comportamiento anómalo

Notificaciones inteligentes ante desviaciones de comportamiento normal, priorizadas según riesgo, criticidad de los activos y contexto operativo.

qualoom®

Inspiring Technology
for People

Monitorización, auditoría y respuesta a incidentes

Respuesta a incidentes

Los procedimientos deben estar formalizados y automatizados:

01

Definición de playbooks

Procedimientos estandarizados que detallan pasos a seguir para distintos tipos de incidentes, asegurando consistencia y rapidez en la respuesta.

02

Automatización mediante SOAR

Ejecución automática de tareas repetitivas o de bajo riesgo, reduciendo tiempos de reacción y errores humanos.

03

Integración con plataformas SIEM

Consolidación de información de seguridad y operación para permitir análisis centralizado, correlación avanzada y trazabilidad completa de eventos.

Auditoría y trazabilidad

La auditoría asegura control y cumplimiento:

01

Registro inmutable de actividades

Almacenamiento seguro de logs que garantiza integridad, disponibilidad y no repudio, fundamental para auditorías y revisiones regulatorias.

02

Evidencias documentadas para cumplimiento

Información organizada que respalda el cumplimiento normativo y facilita la generación de reportes internos y externos.

03

Análisis forense post-incidente

Investigación estructurada de eventos de seguridad, permitiendo identificar causas raíz, evaluar impacto y definir medidas preventivas futuras.

qualoom®

Inspiring Technology
for People

Buenas prácticas y recomendaciones

La implementación de un modelo de seguridad cloud-native eficaz requiere acciones continuas, integración desde el diseño y mejora iterativa. A continuación se detallan las principales buenas prácticas:

- **Security by Design y Zero Trust:** Incorporar seguridad desde el diseño y validar todos los accesos.
- **Seguridad en CI/CD:** Automatizar análisis de código, escaneo de vulnerabilidades y validaciones de configuración.
- **Revisión de roles y permisos:** Ajustar accesos regularmente para mantener el principio de menor privilegio.
- **Capacitación del equipo:** Actualizar conocimientos en seguridad cloud-native y herramientas.
- **Mejora continua:** Evaluar y ajustar políticas y controles según riesgos y hallazgos de auditoría.

Estas prácticas permiten construir un **entorno cloud seguro, resiliente y alineado con los objetivos de negocio y regulatorios,** garantizando la sostenibilidad y eficacia del modelo de seguridad.

qualoom®

Inspiring Technology
for People

Protege tu nube con seguridad desde el diseño hasta la operación

CONTACTA CON NOSOTROS

www.qualoom.es

contacto@qualoom.es

(+34) 91 236 4808

Más información www.qualoom.es