Guía ejecutiva

Seguridad Cloud

Versión ejecutada — todos los cambios de la revisión aplicados como contenido final.

NOVIS

Tu nube funciona.

Tu control, no.

Los riesgos invisibles de operar en la nube — y el marco que usan las empresas que sí los controlan.

La nube prometió control.

La realidad es otra.

Migrar a la nube resolvió muchos problemas técnicos. También abrió nuevos riesgos que no siempre son visibles.

Hoy, la mayoría de las empresas críticas de Centroamérica operan sobre AWS, Azure, IBM cloud,Google Cloud o entornos híbridos. Dependen de estos entornos para procesos que no pueden detenerse: facturación, banca core, cadena de abasto, atención al cliente.

Sin embargo, pocas pueden responder con certeza:

- quién tiene acceso a qué
- qué configuraciones están activas
- qué tan protegida está realmente su operación

Si tu equipo dudó en alguna respuesta, esta guía es para ti.

Dato ancla
Gartner estima que para 2025, el 99% de las fallas de seguridad en la nube serán responsabilidad del cliente — no del proveedor. Lo que falla no es la nube. Es el modelo con que se opera.

Por qué esta guía
la firma Novis

Esta guía no es teoría. Es lo que hemos visto implementando modelos de control de seguridad en el core tecnológico de empresas de Centroamérica — banca, retail, energía, gobierno, manufactura. Empresas donde una falla de control no es una noticia, son perdidas monetarias.

Lo que nos respalda

- **Trayectoria:** +20 años asegurando infraestructura y aplicaciones críticas en LATAM.
- **Partnerships:** Acuerdos activos con AWS, Microsoft Azure, IBM cloud Google Cloud y SAP.
- **Operación:** Modelo 24×7 con KAM asignado por cliente — no tickets anónimos, no escalamientos perdidos.
- **Enfoque integrador:** Infraestructura, aplicaciones y soporte bajo una sola gobernanza, vs. equipos fragmentados.

5 riesgos que no se ven **hasta que ya hicieron daño**

El problema no suele aparecer como un ataque inmediato.
Se construye poco a poco — hasta que un incidente lo expone.

01- Accesos sin control

Usuarios con permisos innecesarios, cuentas de exempleados activas, falta de MFA en consolas privilegiadas.
52% de las brechas incluyen credenciales comprometidas — Verizon DBIR 2024.

02 - Configuraciones incorrectas

Buckets públicos, reglas de firewall abiertas, servicios expuestos sin intención.
23% de los incidentes cloud reportados — fuente: IBM Cost of a Data Breach 2024.

03 - Falta de monitoreo

Cambios y eventos que pasan desapercibidos por días o meses.
Tiempo medio de detección: 204 días — IBM Cost of a Data Breach 2024.

04 - Dependencia de terceros

Operación distribuida en proveedores y SaaS sin control central.
29% de las brechas involucran un tercero — Verizon DBIR 2024.

05 - Respuesta lenta ante incidentes

Sin runbooks definidos, cada incidente es improvisación — y la improvisación cuesta tiempo.
Costo promedio de una hora de downtime en empresas medianas LATAM: USD 15,000+ — Gartner.

Caso ilustrativo

Un banco regional descubrió en una auditoría que el 37% de sus cuentas con privilegio administrador pertenecían a personas que ya no trabajaban en la empresa. Ninguna había sido revocada en los 8 meses posteriores a su salida.
No hubo ataque. Hubo suerte.

Cuando el problema aparece, casi

nunca es un hackeo

En la mayoría de los casos, el impacto no es un ataque mediático.
Es algo más cotidiano:

- interrupciones en la operación
- pérdida o corrupción de información
- errores en sistemas críticos sin posibilidad de revertir
- dependencia total de un proveedor que no responde

El costo real
El costo promedio de una hora de downtime en una empresa mediana de LATAM supera los USD 15,000 (Gartner). En sector financiero, esa cifra puede multiplicarse por 10. **Y eso es solo una hora.**

El problema no es el ataque.
Es no tener control cuando algo sucede.

Y no tener control cuando algo sucede no es mala suerte. Es la consecuencia predecible de no haberlo gobernado antes.

El falso sentido **de seguridad**

La mayoría de las empresas que se sienten seguras en realidad tienen herramientas — no modelo. Estas son las cuatro confusiones más comunes.

Lo que crees	La realidad
Antivirus instalado.	El antivirus no ve lo que pasa en AWS, Azure o Google Cloud.
Usas herramientas de seguridad.	Las herramientas reportan; no deciden por ti.
Estás en AWS / Azure / GCP.	El hyperscaler asegura la plataforma. Tú aseguras lo que corre encima.
Tienes alertas configuradas.	Alertas sin runbook ni dueño = ruido que nadie atiende.

En los proyectos de seguridad cloud que Novis ha acompañado en Centroamérica, 8 de cada 10 empresas tenían herramientas de seguridad. Ninguna tenía un modelo claro de quién actúa cuando se dispara una alerta.

Tener herramientas no es lo mismo que tener visibilidad.

Tener visibilidad no es lo mismo que poder actuar.

De proteger → a gobernar

Aquí cambia el enfoque.

Los tres pilares para

gobernar tu nube

Las empresas con cloud bajo control no usan más herramientas. Usan un modelo. Tres capas que se ciclan continuamente — no se avanza linealmente, se itera.

01 · Visibilidad	02 · Gobernanza	03 · Respuesta
Saber qué existe, quién accede y qué está pasando. Inventario completo, taggeo, monitoreo centralizado, logs unificados en SIEM o CNAPP.	Reglas claras, dueños por servicio, políticas explícitas. La pregunta deja de ser "¿quién decide?" — siempre hay alguien que decide y rinde cuentas.	Runbooks por tipo de incidente, automatización y velocidad. Cuando algo pasa, la respuesta no se inventa: se ejecuta.

Este modelo es compatible con los lineamientos de CIS Controls v8 y NIST Cybersecurity Framework. Novis lo complementa con el modelo de KAM 24×7 e integración SAP/infra que la mayoría de proveedores de seguridad pura no cubre.

¿En qué nivel de **madurez estás?**

La mayoría de las empresas opera entre el nivel 1 y 2. El salto al nivel 3 es donde la seguridad cloud deja de ser reactiva — y donde la mayoría se queda estancada por falta de gobierno, no de tecnología.

NIVEL 1

Reactivo
Se responde cuando duele. No hay inventario completo, los accesos no se revisan, las alertas se atienden cuando alguien tiene tiempo.

NIVEL 2

Preventivo
Hay herramientas instaladas. CIS Benchmark se corre ocasionalmente. Existe MFA en algunas cuentas. Pero falta modelo: cada incidente se resuelve diferente.

NIVEL 3

Controlado
Visibilidad + dueños por servicio + runbooks. La operación es predecible. Los auditores aprueban porque hay evidencia, no promesas.

NIVEL 4

Adaptativo
Automatización, red-teaming continuo, aprendizaje entre incidentes. La seguridad ya no se protege — se entrena.

Cómo empezar:
4 pasos en 90 días

No se trata de hacerlo perfecto. Se trata de empezar a tener control. Estos cuatro pasos son el primer ciclo — el que produce ganancias visibles antes de que termine el trimestre (tiempos aproximados).

PASO 1

Identificar accesos

- **Acción:** Inventario de cuentas con privilegio, eliminar cuentas inactivas +90 días, MFA obligatorio en consolas cloud y SAP.
- **Resultado:** Reducción inmediata de superficie de ataque por credenciales.
- **Tiempo:** Semanas 1–3

PASO 2

Revisar configuraciones

- **Acción:** Ejecutar CIS Benchmarks sobre AWS/Azure/GCP, corregir buckets/storage públicos no intencionales, revisar reglas de firewall.
- **Resultado:** Riesgos de configuración bajan a niveles auditables.
- **Tiempo:** Semanas 3–6

PASO 3

Centralizar monitoreo

- **Acción:** Logs unificados en SIEM o CNAPP, alertas con umbral y dueño, integración con SAP cuando aplique.
- **Resultado:** Las alertas dejan de ser ruido — cada una tiene a alguien que actúa.
- **Tiempo:** Semanas 6–9

PASO 4

Definir responsables

- **Acción:** Matriz RACI por servicio cloud, runbooks por tipo de incidente, cadencia mensual de revisión.
- **Resultado:** Cuando algo pasa, no hay improvisación. Hay protocolo.
- **Tiempo:** Semanas 9–12

Qué medir: los 4 KPIs
que no pueden faltar

Un programa de seguridad cloud sin métricas es un comité. Estos cuatro indicadores son los mínimos para saber si el modelo está funcionando — y son los que te van a pedir cuando llegue una auditoría seria.

KPI	Qué mide	Cómo se mide	Meta recomendada	Por qué importa
MTTD (Mean Time To Detect)	Tiempo en detectar un incidente	Desde que ocurre hasta que se genera una alerta útil	Críticos: < 1hAltos: < 24h	Si detectas en días, no hay monitoreo activo, solo análisis reactivo
MTTR (Mean Time To Respond)	Tiempo en contener o mitigar	Desde la detección hasta la contención del riesgo	Críticos: < 4–8hAltos: < 24–48h	Refleja qué tan efectiva es la respuesta y los procesos
% Configuración segura (CIS)	Nivel de cumplimiento de baseline	% de controles aplicados en activos críticos	≥ 85% aceptable≥ 90% bueno≥ 95% maduro	Indica exposición estructural a riesgos
MFA en privilegios	Protección de cuentas críticas	% de cuentas privilegiadas con MFA activo	Objetivo: 100%Mínimo: 98%	Es el control más efectivo contra accesos indebidos

KPI	Qué mide	Meta recomendada	Por qué importa
Tiempo de parcheo	Remediación de vulnerabilidades críticas	**< 7 días**	Detectar sin corregir no reduce riesgo
Cobertura de monitoreo	Visibilidad de activos críticos	**≥ 90%**	No puedes proteger lo que no ves

Antes y después de implementar

gobierno cloud

Sin gobierno cloud	Con gobierno cloud
Cada incidente es improvisación.	Hay runbooks por tipo de incidente — la respuesta se ejecuta, no se diseña.
Nadie revoca accesos de ex-empleados.	Hay revisión periódica automática y trazabilidad completa.
Las alertas se acumulan sin atender.	Cada alerta tiene un dueño y un SLA de respuesta.
La auditoría encuentra hallazgos críticos.	La auditoría encuentra evidencia. Y eso cierra hallazgos.
TI y Compliance discuten cada mes.	Comparten métricas y metas — el comité es operativo, no político.

Impacto esperado

Las empresas con modelo de gobernanza cloud reducen entre 20% y 30% el tiempo de respuesta ante incidentes en el primer año. (Validar con casos documentados Novis antes de publicar; ajustar a la cifra defendible si fuera necesario.)

LA CONCLUSIÓN:
la seguridad cloudes liderazgo,
no tecnología

La nube no es el riesgo. Operarla sin gobierno sí lo es.

Las empresas que entienden esto no tienen menos incidentes — tienen los incidentes bajo control. Recuperan tiempo de respuesta, cierran hallazgos de auditoría y dejan de depender del heroísmo de un equipo pequeño cuando algo pasa.

La seguridad no depende de una herramienta, sino de la forma en que se gestiona la infraestructura.

Auto-evaluación: ¿en qué nivel **está tu organización?**

Marca cada afirmación con la que estés de acuerdo. Al final, cuenta cuántas marcaste.

- ☐ Puedo listar en menos de 5 minutos a todos los usuarios con privilegio administrador en mis entornos cloud.
- ☐ Las cuentas de exempleados se revocan automáticamente o se revisan en máximo 7 días después de su salida.
- ☐ Tenemos un runbook escrito de qué hacer ante una brecha de datos — y el equipo lo conoce.
- ☐ Ejecutamos CIS Benchmarks (o equivalente) sobre nuestros entornos cloud al menos una vez por trimestre.
- ☐ MFA está activo en el 100% de las cuentas con privilegio administrador.
- ☐ Cuando se dispara una alerta de seguridad, sé exactamente quién la atiende y en cuánto tiempo.

Cómo interpretar tu resultado

5–6 marcadas:	Tu programa de seguridad cloud está maduro (Nivel 3–4). Busca optimizaciones finas y automatización.
3–4 marcadas:	Tienes bases, pero falta gobierno (Nivel 2). Un diagnóstico Novis identifica los gaps en 2 semanas.
0–2 marcadas:	Estás operando sin gobierno cloud (Nivel 1). Cada mes que pasa es exposición acumulada.

Diagnóstico de

seguridad cloud

Revisemos tu modelo actual y evaluemos los riesgos prioritarios de tu operación.

Agenda tu diagnóstico

NOVIS