

Preparando a su organización para la nueva era de la ciberseguridad

La LOFC ya está vigente

Ecuador cuenta con un marco integral de ciberseguridad. La ley introduce nuevas expectativas de gobierno, gestión de riesgos, respuesta a incidentes y resiliencia para las entidades dentro de su alcance.



Desafíos y oportunidades de la LOFC

01

Alcance y regulación

Determinar si la organización está o podría quedar comprendida, y monitorear la normativa secundaria, los estándares mínimos y el Catálogo Nacional.

02

Gobierno y gestión de riesgos

Definir roles, supervisión ejecutiva y métricas, conectando riesgos cibernéticos, activos críticos y controles con los objetivos del negocio.

03

Incidentes y resiliencia

Fortalecer la detección, el escalamiento y la notificación de incidentes dentro del plazo aplicable, y asegurar la continuidad de servicios esenciales.

04

Terceros y pruebas de seguridad

Gestionar proveedores críticos y servicios digitales, y alinear las pruebas de seguridad y Ethical Hacking con el nuevo marco.

Tres datos que ponen la regulación en perspectiva

72 h

Notificación de incidentes relevantes, cuando corresponda.

1,5%

Sanción máxima sobre volumen de negocio, según gravedad.

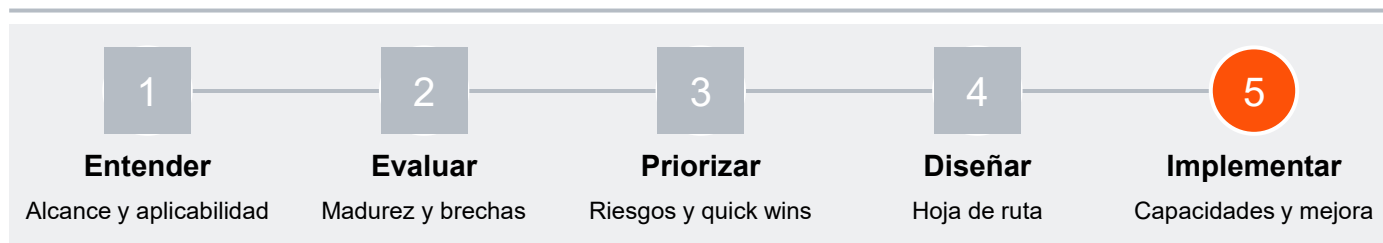
3 grupos

Sector público relevante, infraestructura crítica y servicios digitales.

¿Está preparada su organización?

01	¿Sabe si la LOFC aplica hoy o podría aplicar con el nuevo Catálogo?	02	¿Existe un gobierno claro para supervisar riesgos, controles y terceros?	03	¿La organización puede detectar, escalar y reportar un incidente a tiempo?	04	¿Cuenta con continuidad, respuesta a incidentes y resiliencia probadas?	05	¿Sus proveedores de pruebas de seguridad cumplen el nuevo marco?
----	---	----	--	----	--	----	---	----	--

Enfoque de PwC



Nuestros servicios

Diagnóstico de aplicabilidad LOFC Conclusión de aplicabilidad y mapa preliminar de obligaciones.	01	Cybersecurity Gap Assessment Matriz de brechas, quick wins y hoja de ruta priorizada.	02	Gobierno, riesgos y resiliencia Diseño e Implementación del modelo objetivo, roles, políticas, métricas y planes requeridos.	03
Preparación y respuesta a incidentes Protocolos, playbooks, simulaciones y criterios de notificación.	04	Capacidades complementarias Ethical Hacking, gestión de terceros, cloud, IAM, vulnerabilidades, cultura cyber y servicios gestionados de ciberseguridad.	05	Acompañamiento de implementación Apoyo para ejecutar, monitorear y mejorar las capacidades priorizadas.	06

Conversemos sobre el primer paso para su organización

Patricio Ramón
Socio de Risk Assurance
patricio.ramon@pwc.com

Fernando Fernández
Senior Manager Digital Risk
fernandez.fernando@pwc.com