Elier Alfaro Alfonso.

CISO en Banco BICE - Ingeniero en Computación e Informática. MBA.

Más de 20 años de experiencia profesional en Ciberseguridad.

Certificaciones de Ciberseguridad & Cloud Computing:

1. CISSP (Certified Information Systems Security Professional) – ISC2.
2. CISSP – ISSMP (Information System Security Management Professional) – ISC2.
3. CISM (Certified Information Security Manager) - ISACA.
4. CCSP (Certified Cloud Security Professional) – ISC2.
5. CCSK (Certificate of Cloud Security Knowledge v.4) – Cloud Security Alliance.
6. AWS Certified Solutions Architect – Associate.
7. AWS Certified Cloud Practitioner.

https://www.linkedin.com/in/elier-alfaro-023bb521/

elier-alfaro@outlook.com

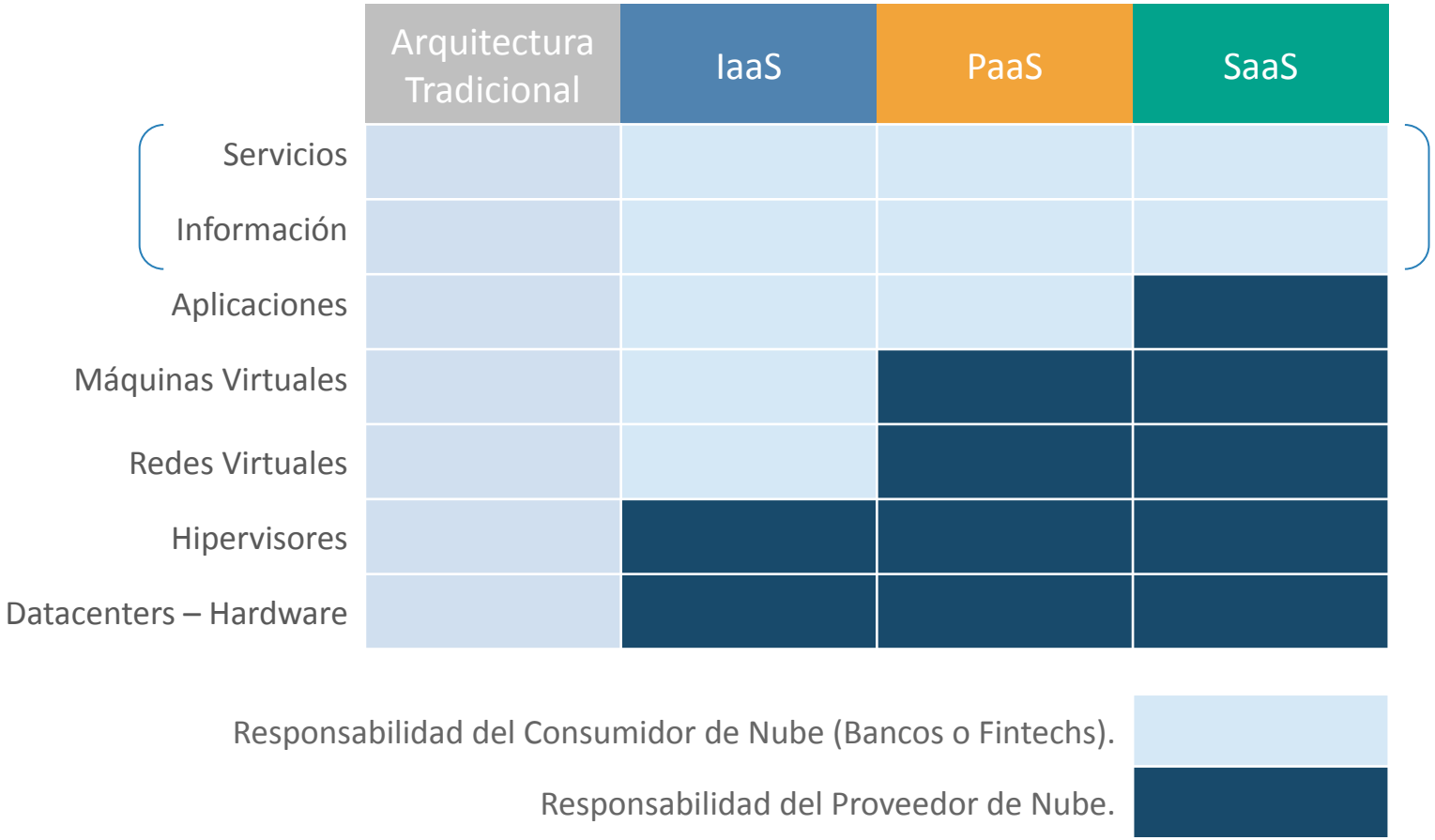
Seguridad en la nube bancaria: ¿qué tan segura es?

Elier Alfaro | MBA | CISSP - ISSMP | CISM | CCSP | CCSK | AWS Certified Solutions Architect – Associate.

Conceptos

Modelos de Servicio de Nube	IaaS (Infraestructure as a Service)	PaaS (Platform as a Service)	SaaS (Software as a Service)
	Servidores virtuales.	Servicios gestionados por el proveedor de nube.	Aplicaciones – Ej: Office 365.
	Modelo de Responsabilidad Compartida.		

Matriz de Responsabilidades

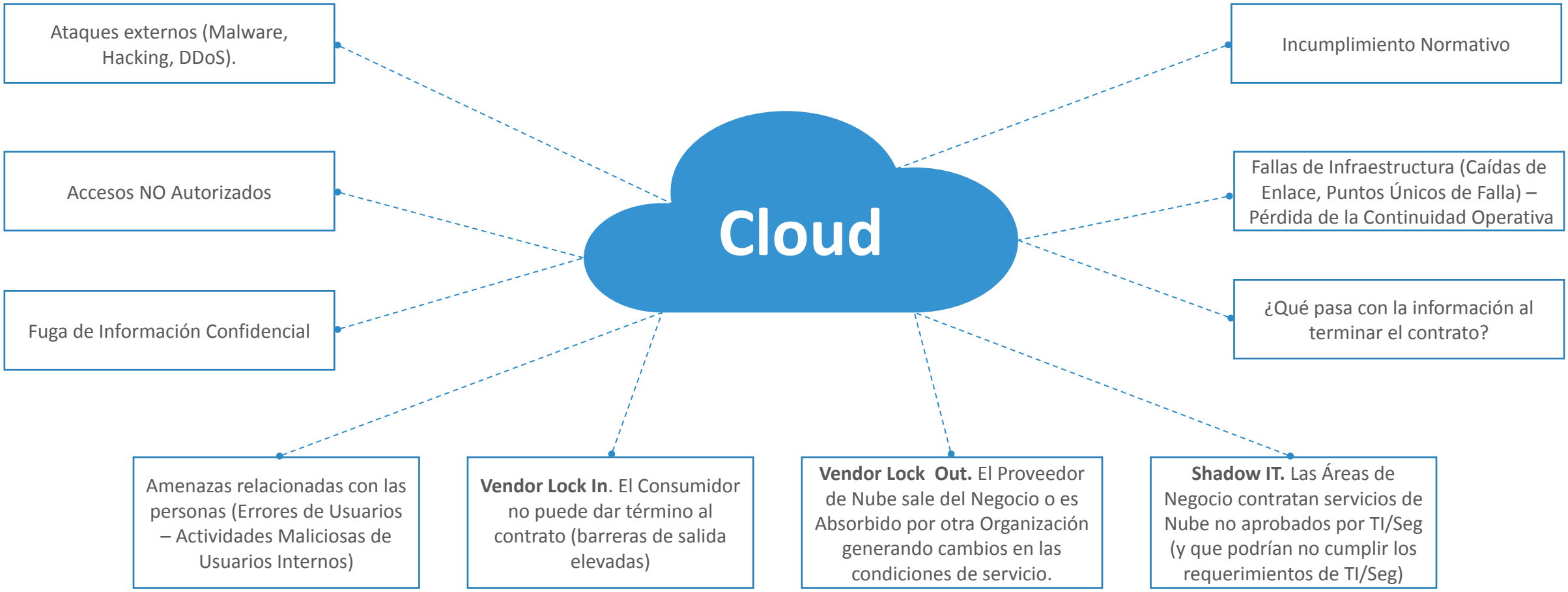


El Accountability frente a los Clientes por la protección de la información y la continuidad de los servicios es siempre del Consumidor de Nube…

Conceptos

Modelos de Servicio de Nube	IaaS (Infraestructure as a Service)	PaaS (Platform as a Service)	SaaS (Software as a Service)
	Servidores virtuales.	Servicios gestionados por el proveedor de nube.	Aplicaciones – Ej: Office 365.
	Modelo de Responsabilidad Compartida.		
	Adecuada Gestión de Riesgos.		

Principales Riesgos de Seguridad que deben ser gestionados por los Bancos y las Fintechs al utilizar servicios de Nube.



Elier Alfaro | MBA | CISSP - ISSMP | CISM | CCSP | CCSK | AWS Certified Solutions Architect – Associate.

Conceptos

	IaaS (Infraestructure as a Service)	PaaS (Platform as a Service)	SaaS (Software as a Service)
Modelos de Servicio de Nube	Servidores virtuales.	Servicios gestionados por el proveedor de nube.	Aplicaciones – Ej: Office 365.
	Modelo de Responsabilidad Compartida.		
	Adecuada Gestión de Riesgos.		
Casos de Uso Relevantes para la presentación	Los Bancos (o las Fintechs) utilizan grandes proveedores de nube, como AWS, Microsoft, Google u otros, para ofrecer servicios a sus clientes.		Los Bancos (o las Fintechs) son Clientes aplicaciones SaaS.
Control de la Seguridad	Los Bancos (o las Fintechs) puede lograr excelentes niveles de seguridad. Siempre que se usen los grandes proveedores de nube y se sigan las buenas prácticas de configuración, recomendadas por los proveedores de nube.		Los Bancos (o las Fintechs) ceden el control de la seguridad de la aplicación SaaS al Proveedor. Preocupaciones: ¿Dónde se almacena la información? ¿Cómo se protege?
Objetivos de la Sesión	Comentar las funcionalidades de nube que pueden ser utilizadas por los Bancos (o las Fintechs) para lograr altos estándares de seguridad y resiliencia.		Entregaremos recomendaciones de como gestionar proveedores SaaS.

Algunas Funcionalidades de Nube

1 Infraestructura Global.

- Regiones.
- Zonas de Disponibilidad.

Beneficios
• Desplegar recursos globales. • Alta disponibilidad, tolerancia a fallas.

2 Servicios Administrados.

- de red (Balanceadores de Carga, Firewalls).
- de Bases de Datos.
- de Analítica y procesa-miento de datos.
- de almacenamiento.
- de inteligencia artificial.
- Y muchos más…

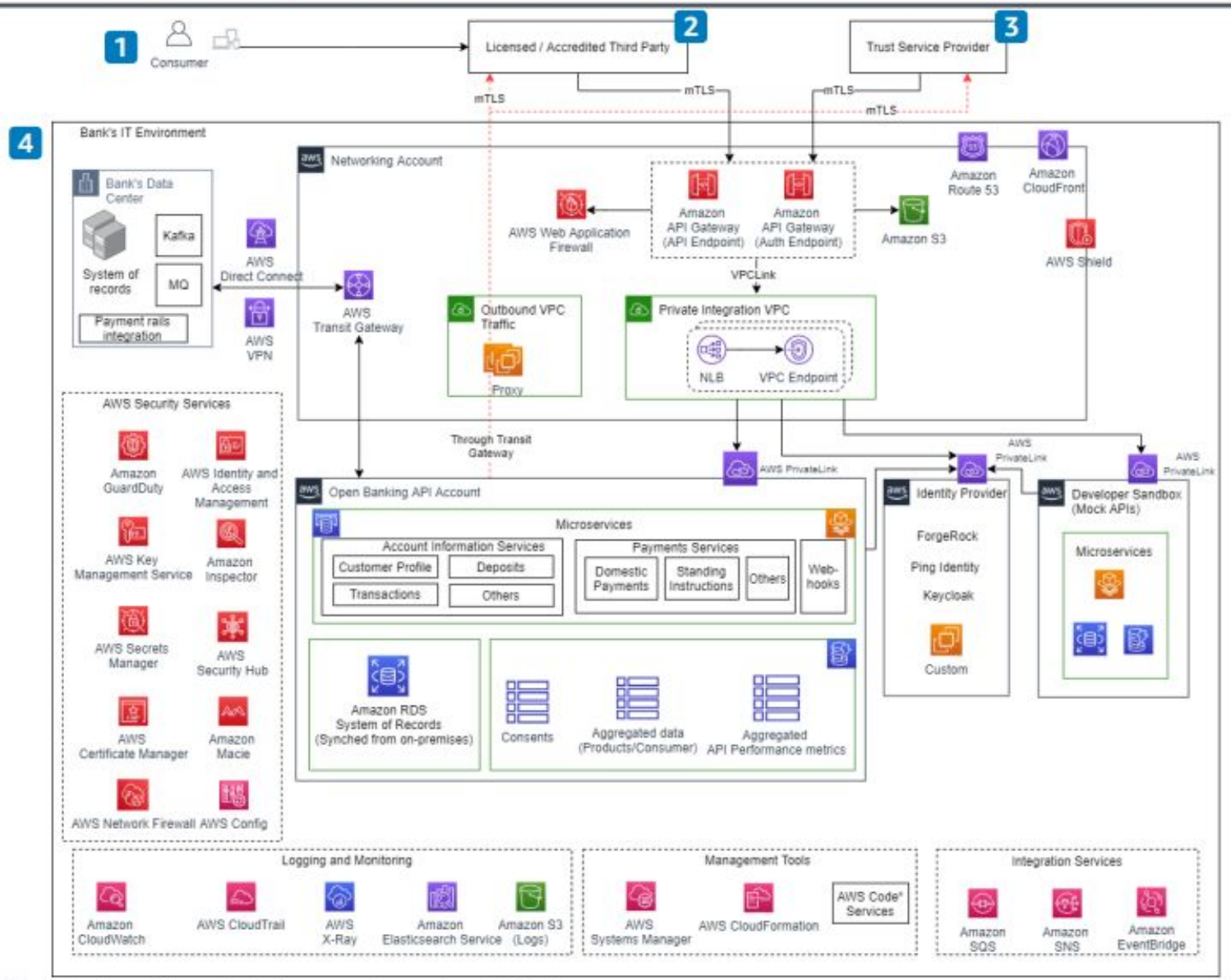
Beneficios
• Mayor disponibilidad y fiabilidad. • Escalabilidad y elastici-dad (Pago por uso). • Mayor seguridad. • Mayor simplicidad, agilidad. • Menores tiempos de gestión.

2 Infraestructura como Código.

- En un archivo de configuración se puede automatizar la configu-ración, el aprovisiona-miento y la gestión de la infraestructura en la nube.

Open Banking on AWS

Use Amazon Web Services to open APIs for third parties and help you implement Open Banking regulations.



Infraestructuras tan complejas como esta, se pueden crear a partir de un archivo que contiene todos los detalles de configuración de los distintos componentes.

Las herramientas de inteligencia artificial pueden ayudarnos en la creación del archivo de configuración.

Reviewed for technical accuracy September 7, 2021

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture

Algunas Funcionalidades de Nube

1 Infraestructura Global.

- Regiones.
- Zonas de Disponibilidad.

Beneficios

- Desplegar recursos globales.
- Alta disponibilidad, tolerancia a fallas.

2 Servicios Administrados.

- de red (Balanceadores de Carga, Firewalls).
- de Bases de Datos.
- de Analítica y procesamien-to de datos.
- de almacenamiento.
- de inteligencia artificial.
- Y muchos más…

Beneficios

- Mayor disponibilidad y fiabilidad.
- Escalabilidad y elasticidad (Pago por uso).
- Mayor seguridad.
- Mayor simplicidad, agilidad.
- Menores tiempos de gestión.

3 Infraestructura como Código.

- En un archivo de configuración se puede automatizar la configuración, el aprovisiona-miento y la gestión de la infraestructura en la nube.

Beneficios

- Permiten recuperarnos ante desastres ocasionados por ciberataques muy rápida-mente.

4 Automatización.

- Se pueden automatizar tares de monitoreo y res-puesta ante amenazas.
- Elasticidad.

Beneficios

- Eficiencia en la seguridad.

5 Servicios de Seguridad.

- Excelentes herramientas de Protección, Detección, Respuesta y Recuperación.
- Monitoreo de postura.
- Inteligencia de amenazas.
- Uso de la inteligencia artificial.

Beneficios

- Mayor seguridad a menores costos.

Las buenas prácticas establecen:

- Implementar servicios distribuidos en varias zonas de disponibilidad.
- Utilizar los servicios administrados por los proveedores de nube (PaaS).
- Utilizar Infraestructura como código y automatización.
- Utilizar los servicios de seguridad que ofrece la nube.
- Utilizar arquitecturas basadas en defensa en profundidad y Zero Trust (no confianza, verificación robusta de identidad y políticas de menor privilegio).
- Prepararse para las fallas y testear los Planes de Continuidad y Recuperación ante Desastres.

Elier Alfaro | MBA | CISSP - ISSMP | CISM | CCSP | CCSK | AWS Certified Solutions Architect – Associate.

Recomendaciones Finales…

Para Servicios (IaaS - PaaS).

- Aplicar robustos mecanismos de control de acceso.
- Utilizar segmentación de redes, de suscripciones.
- Proteger el acceso a la consola (Management Plane). Cuidado con la cuenta root, MFA, menor privilegio.
- Implementar seguridad en todo el ciclo de vida de desarrollo de aplicaciones.
- Seguir las buenas prácticas de arquitectura y seguridad, entregadas por los proveedores de nube.
- Utilizar consultores certificados en la nube que se utiliza.

Para Aplicaciones SaaS

- Evaluar los riesgos antes mencionados e impacto para el Negocio.
- Utilizar proveedores con Certificación SOC2 Tipo 2.
- Implementar un monitoreo continuo de la postura de seguridad.
- Considerar barreras de salida y que sucede con la información cuando termina el servicio.
- El contrato con el proveedor debe establecer sólidos compromisos relacionados con la seguridad y privacidad de la información; la notificación ante incidentes de seguridad y la posibilidad de auditar.
- MFA e Integración con Active Directory de la Organización.

Conclusión

La nube bancaria puede ser MUY SEGURA si es bien implementada…

MUCHAS GRACIAS…

Elier Alfaro Alfonso.

CISO en Banco BICE - Ingeniero en Computación e Informática. MBA.

Más de 20 años de experiencia profesional en Ciberseguridad.

Certificaciones de Ciberseguridad & Cloud Computing:

1. CISSP (Certified Information Systems Security Professional) – ISC2.
2. CISSP – ISSMP (Information System Security Management Professional) – ISC2.
3. CISM (Certified Information Security Manager) - ISACA.
4. CCSP (Certified Cloud Security Professional) – ISC2.
5. CCSK (Certificate of Cloud Security Knowledge v.4) – Cloud Security Alliance.
6. AWS Certified Solutions Architect – Associate.
7. AWS Certified Cloud Practitioner.

https://www.linkedin.com/in/elier-alfaro-023bb521/

elier-alfaro@outlook.com