IMPLEMENTAR UN PROGRAMA EFECTIVO DE CIBERSEGURIDAD EN LA NUBE

Luis Moreno & otras IA

UN POCO SOBRE MÍ

Mi carrera inició a los 17 años dando cursos de sistemas operativos y ofimática.

Posteriormente pasé por soporte técnico, administración de centros de cómputo, en el NOC de un ISP, y mi primer empleo 100% dedicado a la seguridad lo obtuve hace unos 15 años implementando ISO 27001. Desde entonces, todos mis empleos han sido relacionados a la seguridad de la información, los últimos 10 han sido muy enfocados al sector financiero, he colaborado con 3 de los 5 Bancos más grandes de México.

Actualmente participo en un proyecto para capacitar gratuitamente a personas de cualquier edad y país (en español) en temas de cyber.

Consejero en una startup de pruebas de penetración

Organizador del Meetup: **Mexico City Cybersecurity**

Me gusta viajar, asistir a conciertos

Mi genero favorito es hip-hop

Cine, series, películas.

Ver y practicar box, tochito.

Aprendiendo producción musical y el idioma alemán

AGENDA

Introducción

Algunas definiciones

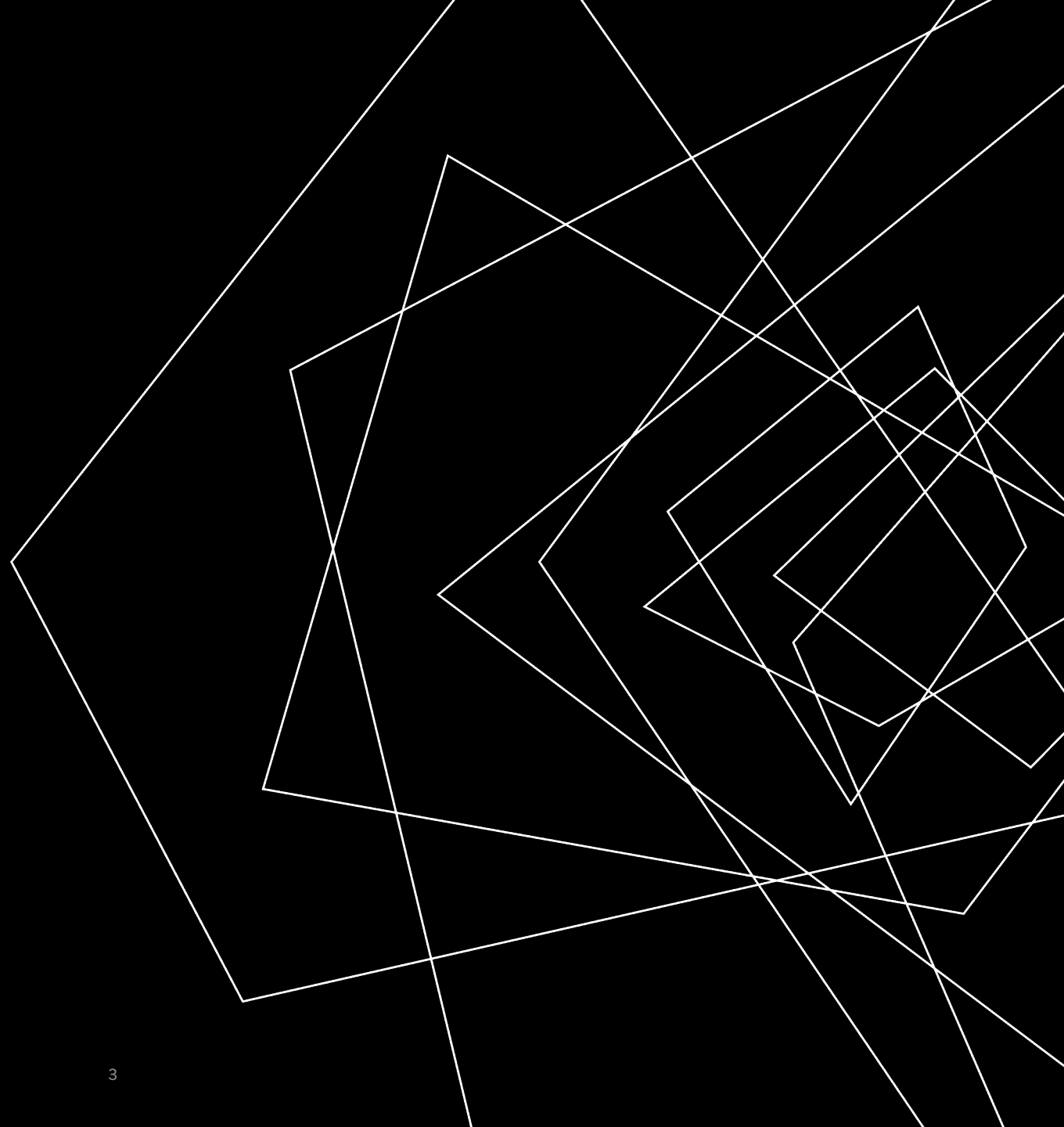
Factor humano

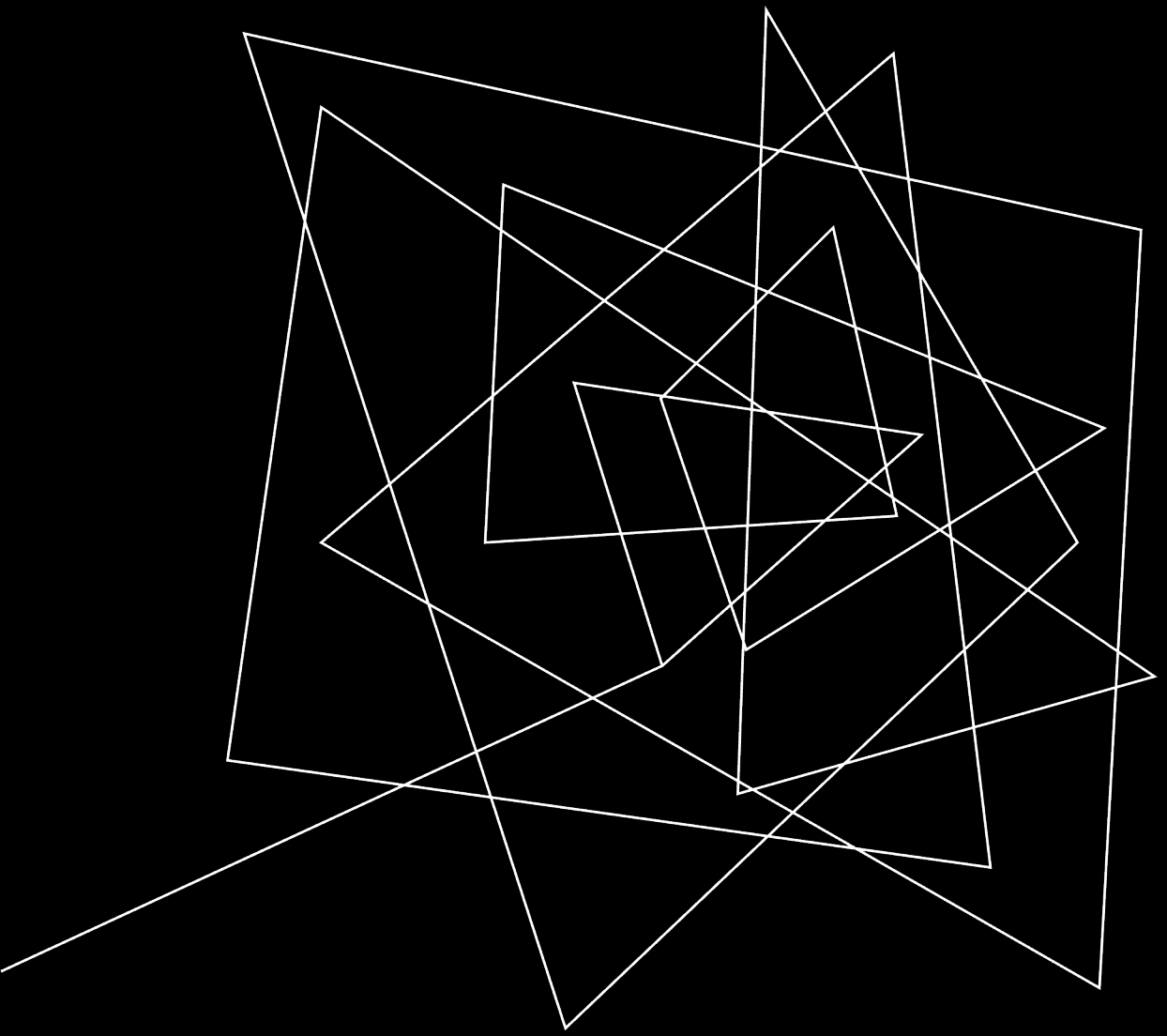
Entendimiento del negocio

Etapas y modelo de madurez

Estándares y marcos de referencia

Puntos clave





PARTE I

Introducción

INTRODUCCIÓN

En esta plática trataré de compartirles algunos puntos clave para implementar un programa efectivo de ciberseguridad holístico y agnóstico en la nube pública, mi experiencia principal es con AWS pero la estrategia, técnicas y procesos pueden ser aplicados para cualquier nube pública similar a AWS y varios incluso a infraestructuras on-premises.

El enfoque del programa es en la seguridad que le corresponde al cliente de la nube pública, en el modelo de seguridad compartida.

Las soluciones son enfocadas a AWS pero pueden ser aplicadas para cualquier otra nube solo haciendo la “traducción”.

La platica está más enfocada a “vanilla Cloud” o herramientas nativas y Open Source.

ALGUNAS DEFINICIONES

Eficiencia: hacer bien las cosas. Es decir, realizar una tarea buscando la mejor relación posible entre los recursos empleados y los resultados obtenidos. La eficiencia tiene que ver con el «cómo». El modelo para la mejora de la eficiencia se apoya en tres pilares básicos: personas, procesos y clientes. Y se logra con personas competentes o con capacidades, actitudes, aptitudes, habilidades y experiencias. Se necesitan flujos rápidos, efectivos y continuos de actividades que añaden valor al producto o al servicio para el cliente con procesos eficientes, analizando dichas actividades y calidad.

Eficacia: hacer las cosas correctas. Es decir, llevar a cabo tareas de la mejor manera, que conduzcan a la consecución de los resultados. Tiene que ver con «qué» cosas se hacen. Eficacia es hacer lo necesario para alcanzar o lograr los objetivos deseados o propuestos.

Efectividad: hacer bien las cosas correctas. Es decir, que las tareas que se lleven a cabo se realicen de manera eficiente y eficaz. Tiene que ver con «qué» cosas se hacen y «cómo».

Basado en ideas de Peter Druker con texto de Forbes: https://www.forbes.com.mx/eficiencia-eficacia-efectividad-son-lo-mismo/

ALGUNAS DEFINICIONES CONT...

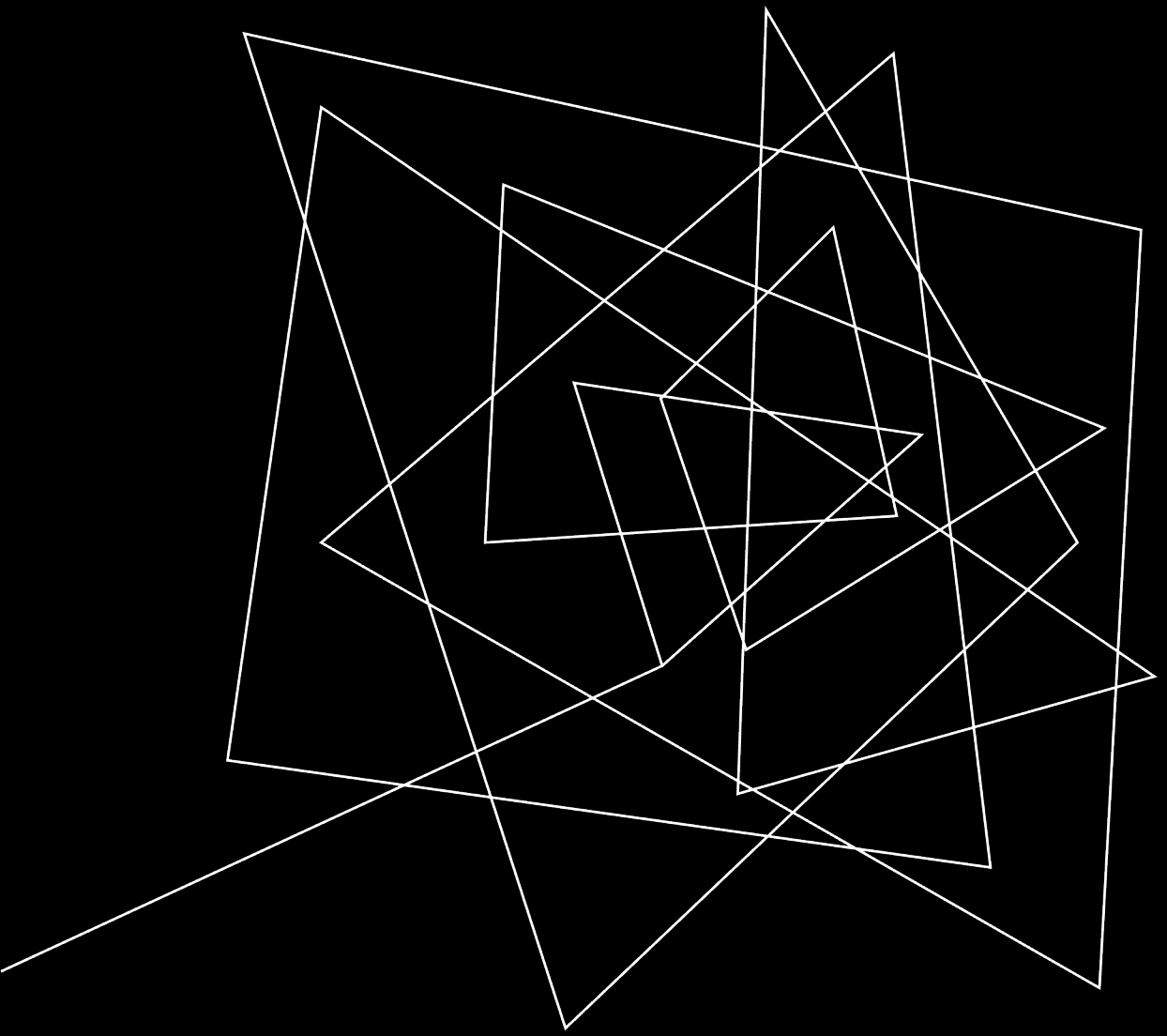
Empatía: La empatía es la capacidad de comprender y compartir los sentimientos, pensamientos y emociones de otra persona, poniéndose en su lugar y experimentando lo que siente desde su perspectiva. La empatía implica ser sensible a las experiencias de los demás, escuchar activamente y mostrar comprensión y apoyo emocional.

Esta habilidad es fundamental en las relaciones interpersonales y en la comunicación efectiva, ya que permite a las personas conectarse emocionalmente y establecer una relación de confianza y respeto mutuo. La empatía es especialmente importante en contextos laborales, educativos y sociales, ya que facilita la colaboración, el trabajo en equipo y la resolución de conflictos.

Apetito de riesgo: El apetito de riesgo se refiere a la cantidad y tipo de riesgos que una organización, individuo o entidad está dispuesta a asumir para alcanzar sus objetivos y metas. Esta disposición a enfrentar riesgos puede variar dependiendo de factores como la naturaleza del objetivo, la industria, el entorno económico y las preferencias personales o corporativas.

Cyber: Cybersegurity, ciberseguridad. La ciberseguridad se refiere a la práctica de proteger los sistemas informáticos, redes, dispositivos y datos de ataques malintencionados, robos, daños o acceso no autorizado. Se trata de un conjunto de medidas y técnicas que se aplican para garantizar la integridad, confidencialidad y disponibilidad de la información digital.

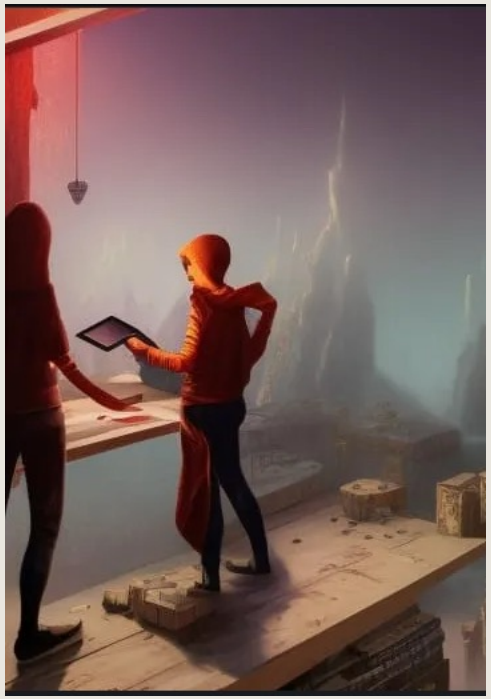
(Según OpenAI, 2021)



PARTE II

El factor humano en la ciberseguridad

EL FACTOR HUMANO DE LA CIBERSEGURIDAD



https://creator.nightcafe.studio/

En la actualidad si preguntamos sobre cuales serían los skills más importantes de un líder en Ciberseguridad ya sea arquitecto, manager, CISO, etc., nos dirán cosas como: networking, desarrollo de software, project managment, Linux, etc., etc. y a pesar de que son skills muy importantes, no es la cualidad que te llevará a implementar programas de seguridad efectivos.

Kha!??

La cualidad más importante de un líder de seguridad en la actualidad es la empatía:

Luis le acabo de preguntar a ChatGPT y ese skill no aparace WTF?

¿Por qué la empatía?

Para empezar El líder de cyber debe estar consciente que

1. No conozco a ninguna organización que solo exista para ser segura, la seguridad solo es parte de, no el todo.

2. Las decisiones que se tomen del lado cyber pueden proporcionar ventaja competitiva o pueden estancar a la organización, dar fidelidad de clientes u odio al producto/servicio.

Aplica también para los clientes internos, usuarios, incidentes de ciberseguridad, hablar con directivos, al interactuar con otras áreas.

DevSecOps es básicamente empatía entre Dev Sec y Ops

EL FACTOR HUMANO DE LA CIBERSEGURIDAD

Getty images

(Según OpenAI, 2021)

Tienes absolutamente razón. La empatía es de hecho una cualidad importante para un líder en ciberseguridad y debería ser incluida en la lista. La empatía permite a los líderes comprender las preocupaciones, necesidades y perspectivas de los miembros de su equipo, colegas y otros interesados. Esta comprensión es crucial para crear un entorno de trabajo inclusivo y de apoyo, fomentar la colaboración y abordar los aspectos humanos de la ciberseguridad.

La empatía es particularmente importante al tratar con incidentes de seguridad, ya que ayuda a los líderes a comprender el estrés y las presiones enfrentadas por las partes afectadas, lo que les permite brindar apoyo y orientación efectivos durante situaciones desafiantes. Además, los líderes empáticos pueden anticipar mejor el comportamiento del usuario y considerar el aspecto humano al diseñar políticas y soluciones de seguridad, lo que en última instancia contribuye a una estrategia de ciberseguridad más efectiva.

Aquí está la lista revisada de cualidades que un líder en ciberseguridad debe poseer:

1. Experiencia técnica
2. Pensamiento analítico
3. Habilidades de comunicación
4. Liderazgo
5. Adaptabilidad
6. Gestión de riesgos
7. Pensamiento estratégico
8. Habilidades para resolver problemas
9. Aprendizaje continuo
10. Empatía

EL FACTOR HUMANO DE LA CIBERSEGURIDAD

Para mi startup yo preferiría a alguien con inteligencia emocional y que tenga el “big picture” de cada dominio de ciberseguridad sobre alguien que tenga un profundo conocimiento técnico pero carezca de inteligencia emocional.

Las personas con inteligencia emocional tienen varios rasgos que las distinguen de aquellas con una menor capacidad para gestionar sus emociones y relaciones interpersonales. Algunos de estos rasgos son:

Autoconocimiento emocional: Las personas con inteligencia emocional tienen una buena comprensión de sus propias emociones, fortalezas y debilidades.

Autorregulación emocional: Son capaces de controlar sus emociones y pensamientos negativos, y de adaptarse a situaciones cambiantes sin perder la calma.

Motivación: Tienen una motivación intrínseca para lograr sus objetivos y una actitud positiva hacia los desafíos y dificultades.

Empatía: Son capaces de comprender las emociones y perspectivas de los demás, lo que les permite establecer relaciones interpersonales más fuertes y significativas.

Habilidades sociales: Tienen habilidades para la comunicación efectiva, la resolución de conflictos, el trabajo en equipo y la negociación, lo que les permite construir relaciones interpersonales saludables y exitosas.

En general, las personas con inteligencia emocional tienen una capacidad superior para manejar sus propias emociones y las emociones de los demás, lo que les permite establecer relaciones interpersonales positivas y tener un mayor éxito en su vida personal y profesional.

EL FACTOR HUMANO DE LA CIBERSEGURIDAD

Cuando líderes de negocio me preguntan: ¿en que tecnología debo invertir para realmente mejorar mi ciberseguridad? mi respuesta siempre es:

Primero invierte en tu gente, en contratar y en desarrollarla, que tengan o desarrollen las características mencionadas anteriormente, de poco sirve que tengas la más avanzada solución SASE, el mejor DLP, si tus equipos no colaboran entre sí, si no hay empatía entre ellos, si tú no eres empático con ellos, trabajan muchas horas sin recompensa ni reconocimiento, viven en constante estrés, no los conoces, etc.

El primer paso es mejorar esa cultura y en segundo lugar viene la parte técnica, si la primera no funciona la segunda no solucionará la primera.

La parte técnica es esencial pero es mucho más fácil aprender una nueva tecnología que aceptar y desarrollar tu inteligencia emocional.

En este aspecto tanto la organización como los colaboradores deben poner de su parte y como en todo, el mejor cambio es el que viene de dentro hacia afuera.

ENTENDIMIENTO DEL NEGOCIO

El entendimiento del negocio es una parte crucial de un apropiado programa de ciberseguridad, ¿Qué hacen por qué lo hacen, hacía dónde va?
¿Cómo podemos proteger algo que no entendemos, si no sabemos hacia dónde quiere ir el negocio?

TI y por lo tanto ciberseguridad son una parte crucial de cualquier empresa, hoy se dice que todas las empresas son empresas de tecnología porque es muy difícil que en la actualidad no hagan uso de ella.

Por lo anterior la ciberseguridad debe estar alineada a los objetivos de negocio, una vez hecho lo anterior, debemos:

1. Identificar los activos críticos
2. Evaluar los riesgos (identificar vulnerabilidades y posibles soluciones)
3. Implementar las soluciones y darle seguimiento
4. Mejorar y repetir

OBTENER APOYO DE ARRIBA HACIA ABAJO

Sin el apoyo del nivel directivo será una batalla que se convertirá en una guerra de guerrillas donde solo habrá bajas de un lado y difícilmente se ganará.

Para ganar el apoyo de la dirección será necesario entre otras cosas:

1.- Demostrar valor al negocio. Ciberseguridad no se debe ”vender” como un mal necesario, se debe cambiar la perspectiva hacia lo que es: un habilitador del negocio, no como un problema técnico si no como un problema de negocio que se puede transformar en una ventaja competitiva, en lugar de una carga para el negocio. Por ejemplo vender que la empresa está certificada en ISO 27001 pues los productos y servicios serán más seguros y eso ayudará a las ventas, que los usuarios puedan abrir cuentas de banco desde sus celulares sin ir a la sucursal, etc.

2.- Alinearse a los objetivos de negocio (como lo comentamos en el slide anterior)

3.- Comunicarse en su propio idioma. No hablar con tecnicismos que no puedan entender, traducir problemas de seguridad complejos en forma que el management pueda comprender, enfocarse en el “bottom line” es decir cuales serían las ventajas financieras, mostrar métricas, gráficas, comparaciones financieras, mejora en la reputación, lo que ellos entiendan y les interese.

4.- Hacer relaciones con el management (la alta gerencia). Directivos de cumplimento, riesgos, líderes de negocio, marketing, a los que les llame la atención cyber, etc. Aprender a jugar tenis y golf no le cae mal a nadie ;)

OBTENER APOYO DE ABAJO HACIA ARRIBA

Ahora bien, también es importante tener el apoyo de los usuarios, líderes de soporte técnico, administradores de sistemas, desarrolladores, etc.

Si solo contamos con el apoyo del alto mando, será otra de esas iniciativas que solo se intentan cumplir porque se deben cumplir, nadie sabe por qué ni para qué, solo se hace porque alguien con jerarquía lo ordena. El viejo adagio de la seguridad es tarea de todos es completamente cierta, ¿qué pasa si tenemos un magnífico plan de cyber y las mejores herramientas pero un usuario le da click a un link de un 0-day?

Analizar si en este contexto se puede cambiar la perspectiva de que los equipos de cyber son los responsables de la seguridad, porque eso es erróneo, sería como decir que los médicos son responsables de que nos enfermemos o accidentemos y que los hiciéramos responsables por ello, los médicos te pueden ayudar a identificar qué virus te está atacando y cómo contrarrestarlo, también a prevenir enfermedades, pero cada uno de nosotros es responsable de su propia salud.

Por otro lado los equipos de cyber siempre tienen inferioridad numérica, de 10 a 1 de 20 a 1 ¿O más?. ¿Qué pasaría si dijéramos, que cada área es responsable de su seguridad y cyber solo está para prevenir y apoyar? Tal vez los equipos verían a cyber con otros ojos y se involucrarían más. Esta estrategia requeriría de un equipo de cyber maduro que sepa apoyar y que no voltee la espalda en venganza tras años de maltrato (-;

Aquí es donde la empatía juega un papel importantísimo, de ambos lados de la ecuación.

OBTENER APOYO DE ABAJO HACIA ARRIBA

¿Cómo podemos conseguir cooperación de la base de la pirámide?

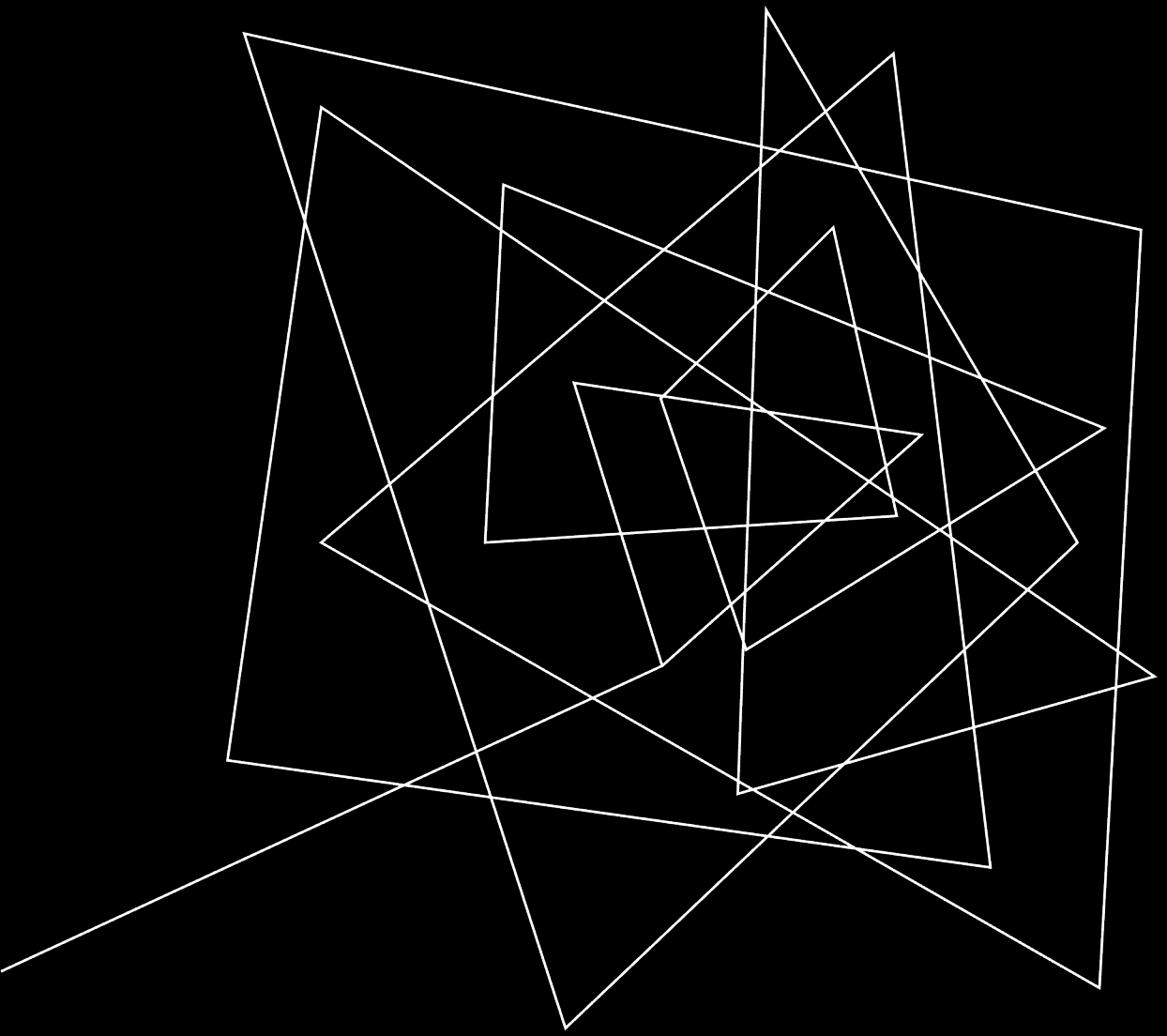
1.- Comunicación. ¿Qué se va a implementar, por qué, para qué y cómo? Explicar de forma tal que cada área comprenda lo que se hará y lo que se espera de ellos. Comunicación constante, no es de una sola vez y recuerda hablar su idioma, cada área es diferente.

2.- Concienciación en ciberseguridad. También conocido como security awareness training donde se ayuda a entender a los usuarios la importancia de la seguridad y como pueden ayudar a proteger los activos de la compañía y su propia información. Es importante que este entrenamiento no sea solo un webinar con algunas preguntas y ya, procurar que sea interactivo, que se muestren demos de cómo un hacker puede comprometerlos a través de phishing, como pueden hacer fuerza bruta a una contraseña débil, esto les ayudará a visualizar el riesgo real y no solo hacer el training porque lo tienen que hacer, ahí no hay ninguna retención, solo es un checkbox.

3.- Conseguir security champions. Personal técnico o no, que tenga mucho interés en el tema de cyber y pueda fungir como promotores de la cultura de seguridad dentro de cada área o equipo de trabajo, esto ayudará a multiplicar a los equipos cyber, tendrá aliados en todas partes.

4.- Asignar una parte del presupuesto para premiar los comportamientos que ayudan a la seguridad, como reportar phishing, identificar posibles riesgos.

Esta parte es esencial pues es imposible tener ojos en todos lados, es mejor contar con aliados.



PARTE III

Procesos y tecnología

MODELO DE RESPONSABILIDAD COMPARTIDA

En este modelo se dice que el CSP (Cloud Service Provider) o el proveedor de servicio de nube es el encargado de la seguridad **DE LA nube** y el CC (Cloud Consumer) o el consumidor o cliente de nube se encarga de la seguridad **DENTRO de la nube**.

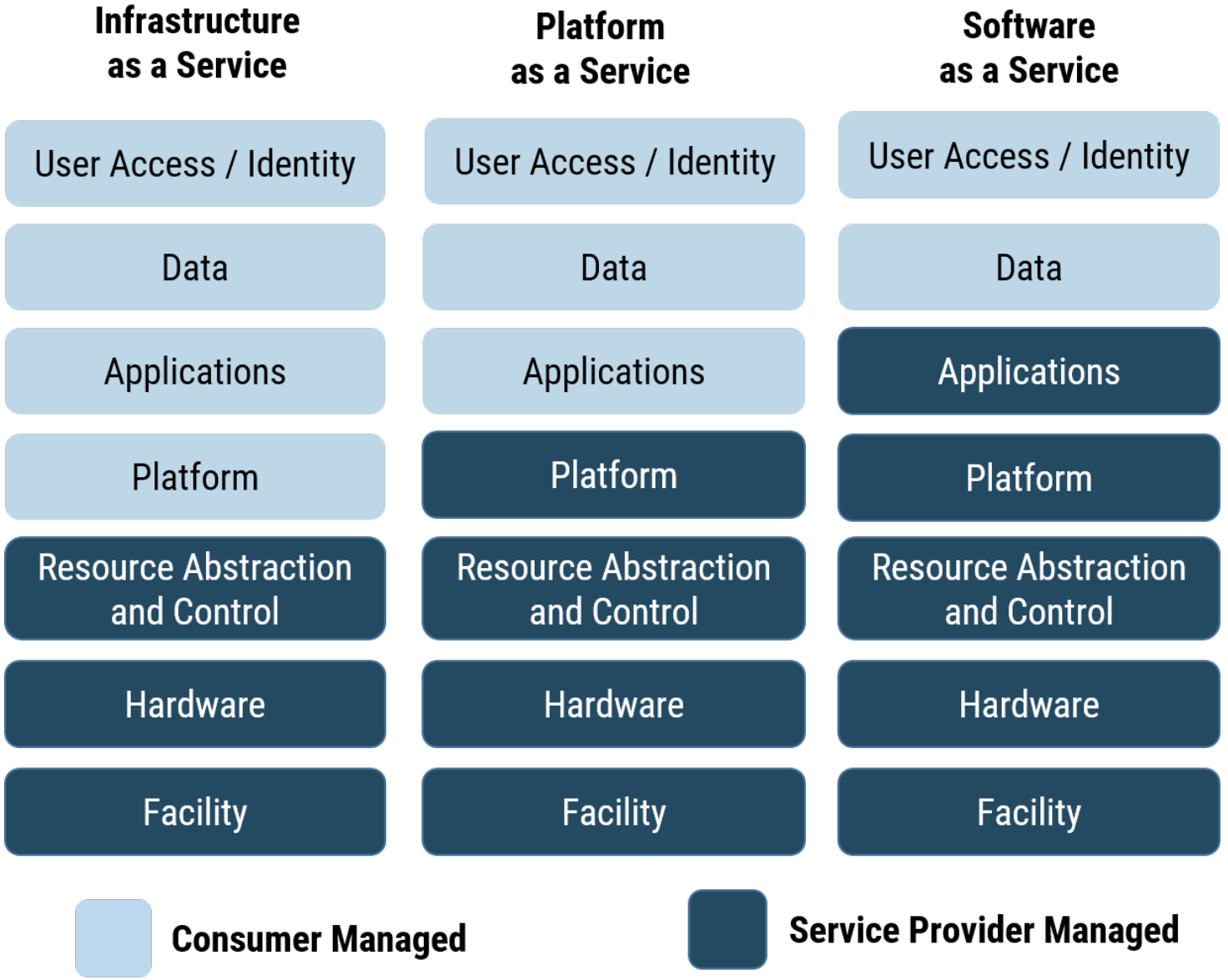


Imagen: Canadian Centre for Cyber Security

IDENTIFICAR ACTIVOS CRÍTICOS

1.- Consultar a los interesados: Consulte con los departamentos clave y los interesados para identificar los activos críticos de la organización desde su perspectiva.

2.- Identificar la información crítica: Identifique la información crítica que es esencial para la organización. Esto puede incluir información de clientes, propiedad intelectual, información financiera, entre otros.

3.- Identificar los sistemas críticos: Identifique los sistemas críticos que son esenciales para la operación de la organización. Esto puede incluir sistemas de gestión de inventario, sistemas de facturación, sistemas de control de acceso, entre otros.

4.- Identificar los procesos críticos: Identifique los procesos críticos de la organización que son esenciales para su operación. Por ejemplo, los procesos de producción, los sistemas financieros o la gestión de la cadena de suministro.

5.- Evaluar la interdependencia: Evalúe cómo se relacionan los activos críticos entre sí y cómo su interrupción afectaría la operación general de la organización.

NIST SP 800-30: Guide for Conducting Risk Assessments
ISO/IEC 27005: Information Security Risk Management
FAIR (Factor Analysis of Information Risk)

Con algunos ajustes a
OpenAI, 2021

PLANEAR UNA ESTRATEGIA GRADUAL DE LARGO PLAZO

Gobierno de la seguridad	Asignar los contactos de Seguridad Seleccione la(s) región(es)
Aseguramiento de la seguridad	Automatizar alineamiento con mejores prácticas con AWS Security Hub
Gestión de identidades y accesos	Autenticación Multi-Factor Evitar el uso de Root y auditarlo Análisis de accesos y roles con IAM Access Analyzer
Detección de amenazas	Detección de amenazas con Amazon GuardDuty y revisar sus hallazgos Auditoría de las llamadas a APIs con AWS CloudTrail Remediar los hallazgos de seguridad en AWS Trusted Advisor Alarma de Billing para detección de anomalías
Gestión de vulnerabilidades	
Protección de la infraestructura	Limitar Security Groups
Protección de Datos	Amazon S3 Block Public Access Analizar la postura de seguridad de datos con Amazon Macie
Seguridad de las aplicaciones	AWS WAF con reglas gestionadas
Respuesta a incidentes	Actuar ante los hallazgos de Amazon GuardDuty

Gatear:

En esta sección veremos funcionalidades o configuraciones sencillas de realizar o habilitar, que aportan mucho valor para reforzar la seguridad. Los “Quick Wins” o “Low hanging fruit”. Son todas recomendaciones que pueden ser implementadas en menos de una semana y lograr muchas mejoras en su postura de seguridad.

Este recurso lo puedes encontrar aquí:

https://maturitymodel.security.aws.dev/es/

PLANEAR UNA ESTRATEGIA GRADUAL DE LARGO PLAZO

Caminar:

En esta sección (Fundacional) se encuentran controles y recomendaciones que pueden llevar algo más de esfuerzo implementar, pero son muy importantes.

Gobierno de la seguridad	Identificar requerimientos de seguridad y regulatorios Plan de entrenamiento sobre seguridad en la nube
Aseguramiento de la seguridad	Monitoreo de las configuraciones con AWS Config
Gestión de identidades y accesos	Repositorio Central de usuarios Políticas Organizacionales - SCPs
Detección de amenazas	Investigar la mayoría de los hallazgos de Amazon GuardDuty
Gestión de vulnerabilidades	Gestiona las vulnerabilidades en tu infraestructura y realiza pentesting Gestiona las vulnerabilidades en tus aplicaciones
Protección de la infraestructura	Gestión de instancias con Fleet Manager Segmentación de redes (VPCs) - Redes Públicas/Privadas Gestión multicuenta con AWS Control Tower
Protección de Datos	Cifrado de Datos - AWS KMS Backups Descubrimiento de datos sensibles con Amazon Macie
Seguridad de las aplicaciones	Involucre a los equipos de seguridad en el desarrollo Sin Secretos en Código - AWS Secrets Manager
Respuesta a incidentes	Definir playbooks de respuesta ante incidentes - Ejercicios TableTop Redundancia en múltiples zonas de disponibilidad

PLANEAR UNA ESTRATEGIA GRADUAL DE LARGO PLAZO

Gobierno de la seguridad	Realizar un modelado de amenazas
Aseguramiento de la seguridad	Crea tus reportes para cumplimiento (como PCI-DSS)
Gestión de identidades y accesos	Revisión de privilegios (Least Privilege) · Estratégia de etiquetado · Customer IAM: Seguridad de tus clientes
Detección de amenazas	Integración con SIEM/SOAR · Análisis de flujos de red (VPC Flow Logs)
Gestión de vulnerabilidades	Security Champions en Desarrollo
Protección de la infraestructura	Pipeline de generación de Imagenes · Anti-Malware / EDR · Control de tráfico saliente · Uso de servicios Abstractos
Protección de Datos	Cifrado en tránsito
Seguridad de las aplicaciones	WAF con reglas custom · Shield Advanced: Mitigación avanzada de DDoS
Respuesta a incidentes	Automatizar Playbooks críticos y los que se ejecutan más frecuentemente · Automatizar configuraciones con corrección de desvíos · Uso de infraestructura como código (CloudFormation, CDK)

Correr:

En la presente etapa (Eficiente) están los controles y recomendaciones que nos permiten gestionar la seguridad en un modo eficiente.

PLANEAR UNA ESTRATEGIA GRADUAL DE LARGO PLAZO

Volar:

En esta sección (Optimizada) las organizaciones están en la vanguardia de la adopción de la nube de AWS y están experimentando con las últimas tecnologías y servicios de seguridad de AWS. En esta fase, las organizaciones están impulsando la innovación en seguridad y liderando el camino en la protección de sus activos digitales.

Gobierno de la seguridad	Conformar un equipo de Ingeniería del Caos (Resiliencia) Compartir la labor y responsabilidad de seguridad
Aseguramiento de la seguridad	
Gestión de identidades y accesos	Control de accesos según el contexto Pipeline de generación de Políticas de IAM
Detección de amenazas	Amazon Fraud Detector Integración de feeds de inteligencia adicionales
Gestión de vulnerabilidades	
Protección de la infraestructura	Estandarización de procesos con Service Catalog
Protección de Datos	
Seguridad de las aplicaciones	DevSecOps Conformación un Red Team (Punto de vista del atacante)
Respuesta a incidentes	Automatizar la mayoría de los Playbooks Amazon Detective: Análisis de causa raíz Conformación un Blue Team (Respuesta ante incidentes) Automación del Disaster Recovery multi-región

OTROS FRAMEWORKS COMO GUÍAS

Además de la estrategia mencionada anteriormente la Cloud Security Alliance (CSA) cuenta con un framework o marco de referencia que está bastante completo, el llamado Cloud Control Matrix (CCM) que la CSA lo define así:

“Está compuesto por 197 objetivos de control que están estructurados en 17 dominios que cubren todos los aspectos clave de la tecnología en la nube. Puede ser utilizado como una herramienta para la evaluación sistemática de una implementación en la nube y proporciona orientación sobre qué controles de seguridad deben ser implementados por cada actor dentro de la cadena de suministro en la nube. El marco de controles está alineado con la Guía de Seguridad para la Computación en la Nube de la CSA y se considera un estándar de facto para la seguridad y cumplimiento en la nube.”

Es muy completo porque tiene todo lo necesario para iniciar con el programa de ciberseguridad, desde los cuestionarios para poder extraer un baseline de cuál es la postura actual y las guías de implementación de los diversos controles, es agnóstica de marcas o nubes y tiene mapeos a ISO 27001, 27002, 27017, 27018, CIS CSC, NIST CSF.

Aquí lo importante es extraer los dominios que pertenecen al CSP y seleccionar los dominios que aplican para la organización en particular.

https://cloudsecurityalliance.org/research/cloud-controls-matrix/

OTROS FRAMEWORKS COMO GUÍAS

Which security domains are covered by the CCM?

A&A	Audit and Assurance
AIS	Application & Interface Security
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control and Configuration Management
CEK	Cryptography, Encryption and Key Management
DCS	Datacenter Security
DSP	Data Security and Privacy
GRC	Governance, Risk Management and Compliance
HRS	Human Resources Security
IAM	Identity & Access Management
IPY	Interoperability & Portability
IVS	Infrastructure & Virtualization Security
LOG	Logging and Monitoring
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management
UEM	Universal EndPoint Management

OTROS FRAMEWORKS COMO GUÍAS

¿Cuánto cuesta el framework de la CSA?

Licensing the CCM or CAIQ

CSA offers licensing opportunities for organizations interested in leveraging the CCM and CAIQ for commercial exploitation. CSA Executive and Corporate members receive a discount on 1 year, 2 year, 5 year, and 10 year licensing contracts. Non members can also license the CCM or CAIQ at an increased price.

When Do I Need a License?

You will need a license if you plan to use the CCM or CAIQ in products and services that are sold to the public. Examples of products and services are:

- Software based products such as 3rd party risk assessment solution and other tools.
- Services, such as consultancy assessment methodologies, audits and evaluation approaches, etc.

You don't need a license if you are just using the CCM for internal purposes.

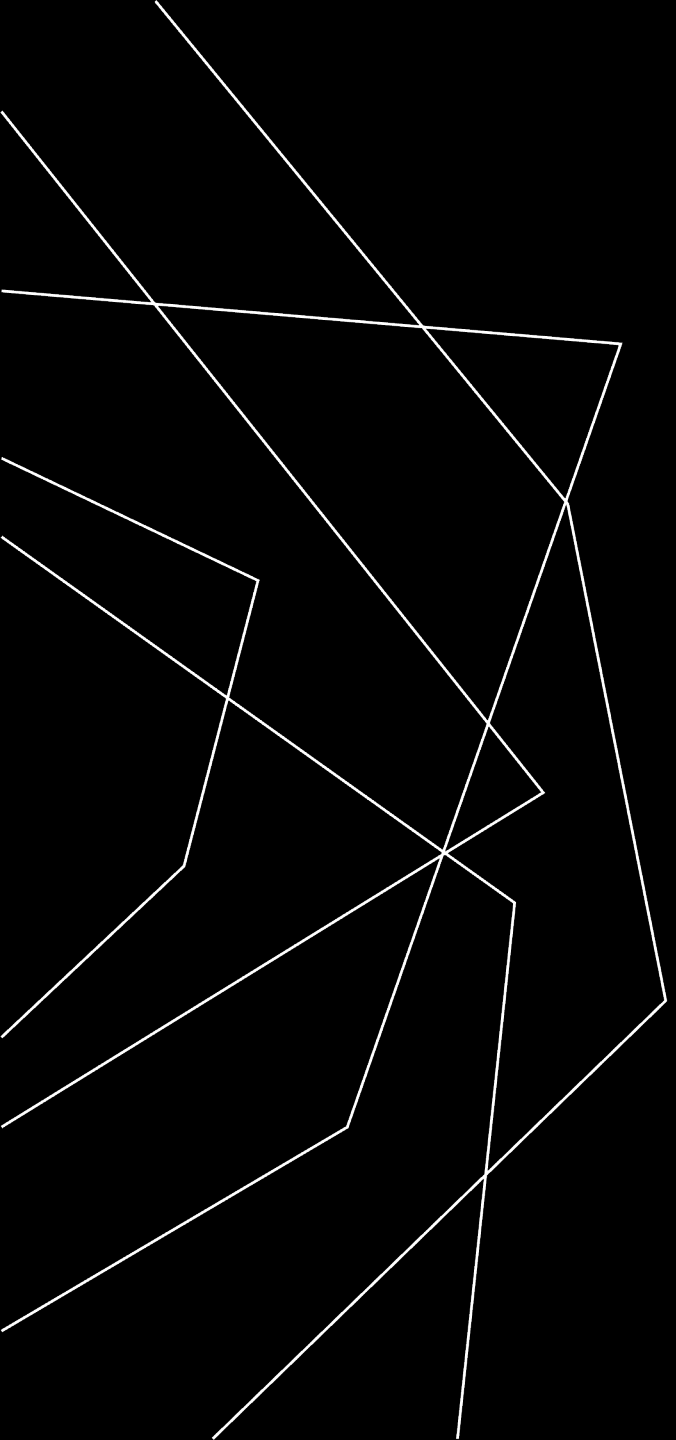
CONSIDERACIONES IMPORTANTES

- **Entrenamiento y práctica** (A Cloud Guru, Whizlabs, AWS)
- Incluir ciberseguridad desde la arquitectura y el diseño del proyecto
- Usar llaves lo menos posible, (preferir assume role en lugar de múltiples llaves)
- MFA everywhere, incluso en el CLI https://repost.aws/knowledge-center/authenticate-mfa-cli
- Usar AWS Vault para protección contra ransomware
- Automatizar lo más posible
- Usar Infrastructure as Code (IaC) desde el inicio
- Tagging
- Guardrails con SCP – Service Control Policies
- Alarma de Billing

Madurar hacía:

- BYOK – Bring your own key
- Zero Trust

https://cloudsecurityalliance.org/research/cloud-controls-matrix/



¡GRACIAS!

Luis Moreno

luis.moreno@hackvolution.io

www.luismoreno.io

EJEMPLO SCP

Evitar que los usuarios desactiven CloudWatch o alteren su configuración

Un operador de CloudWatch de con bajos privilegios necesita monitorear paneles y alarmas. Sin embargo, el operador no debe poder eliminar ni cambiar ningún panel o alarma que las personas con privilegios elevados hayan establecido. Esta Política de Control de Servicio (SCP) evita que los usuarios o roles en cualquier cuenta afectada ejecuten cualquiera de los comandos de CloudWatch que puedan eliminar o cambiar los paneles o alarmas.

```
{ "Version": "2012-10-17",
  "Statement": [
     {
        "Effect": "Deny",
        "Action": [
           "cloudwatch:DeleteAlarms",
           "cloudwatch:DeleteDashboards",
           "cloudwatch:DisableAlarmActions",
           "cloudwatch:PutDashboard",
           "cloudwatch:PutMetricAlarm",
           "cloudwatch:SetAlarmState"
        ],
        "Resource": "*"
     }
  ]
}
```

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_cloudwatch.html#example_cloudwatch_1