TECNOLÓGICO SUPERIOR CORDILLERA

25 AÑOS

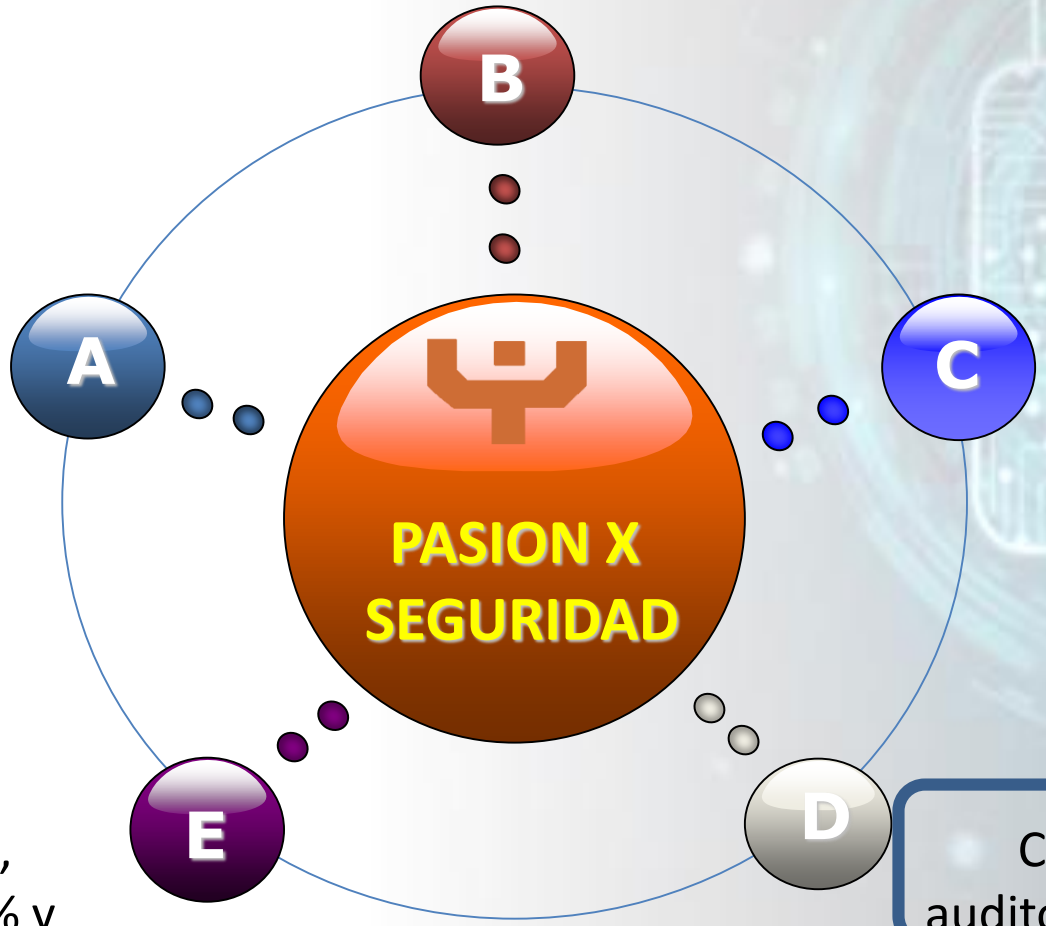
CIDE
Centro de Investigación y Desarrollo Ecuador

SEMINARIO INTERNACIONAL DE SEGURIDAD EN EL DESARROLLO DE SOFTWARE

MSc. Ing. Guido Rosales

GUIDO ROSALES URIONA

Maestrias en Redes (Aviacion Civil) y Direccion Estrategica de TI



Ing. Sistemas
xURSS

Certificaciones
CISA, CISM, LA 27001,
CBS, CISO, ISSA, CSSH

Facilitador 60%,
conferencista 30% y
Docente Universitario
10%

Consultor en Seguridad,
auditorias y FORENSE (50-20-30)

MSc. Ing. Guido Rosales

Desde el año 1999

Yanapti

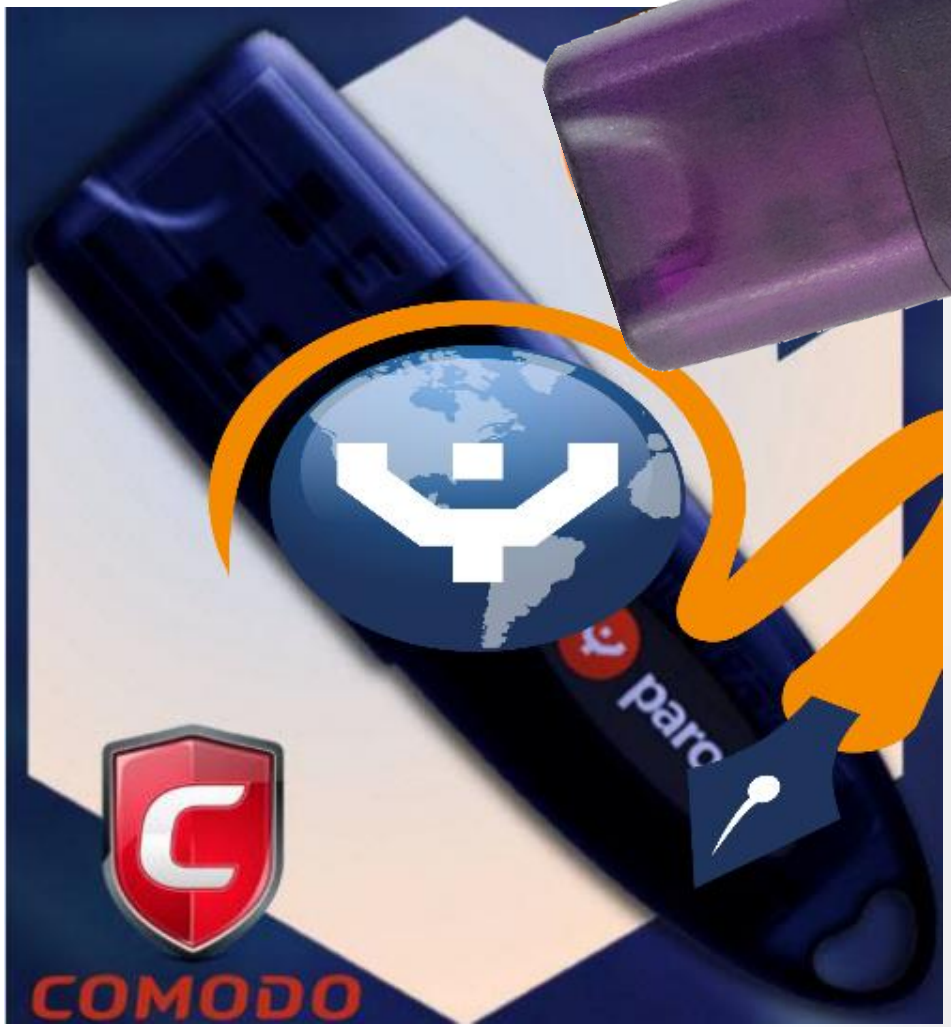
CYBERSECURITY

MSc. Ing. Guido Rosales

09:00 – 09:30	PROGRAMA DE INAUGURACIÓN	
09:30 – 11:00	**CONFERENCIA MAGISTRAL DE APERTURA:** Desarrollo seguro en el contexto de la Seguridad Ágil **Expositor:** Ing. Guido Rosales Uriona **Yanapti SRL - Bolivia**	

QUE ES UNA FIRMA DIGITAL?

MSc. Ing. Guido Rosales


COMODO


ePass2003Auto

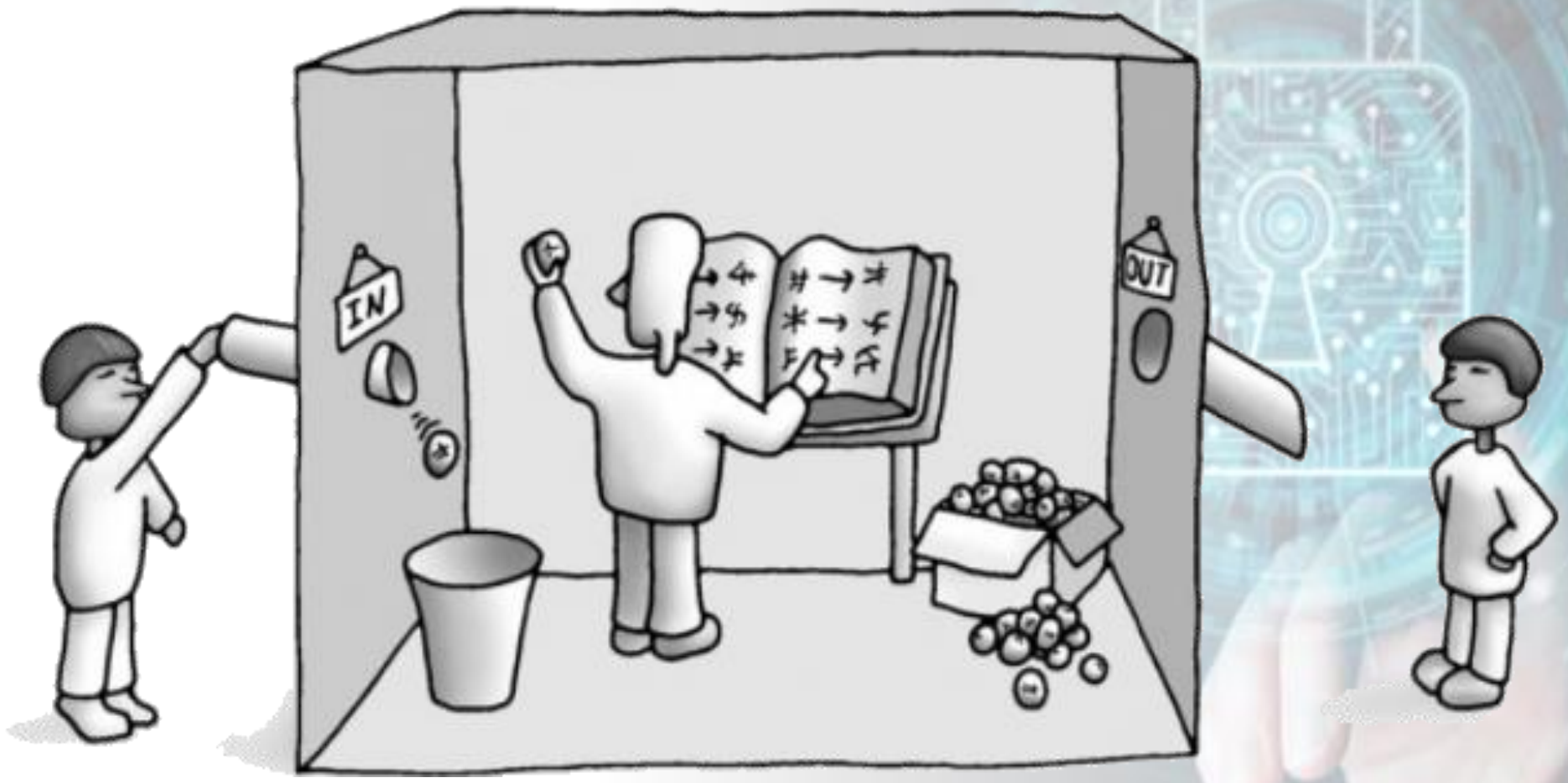

CORP

SOFTWARE FACTORY – FABRICACIÓN DEL SOFTWARE

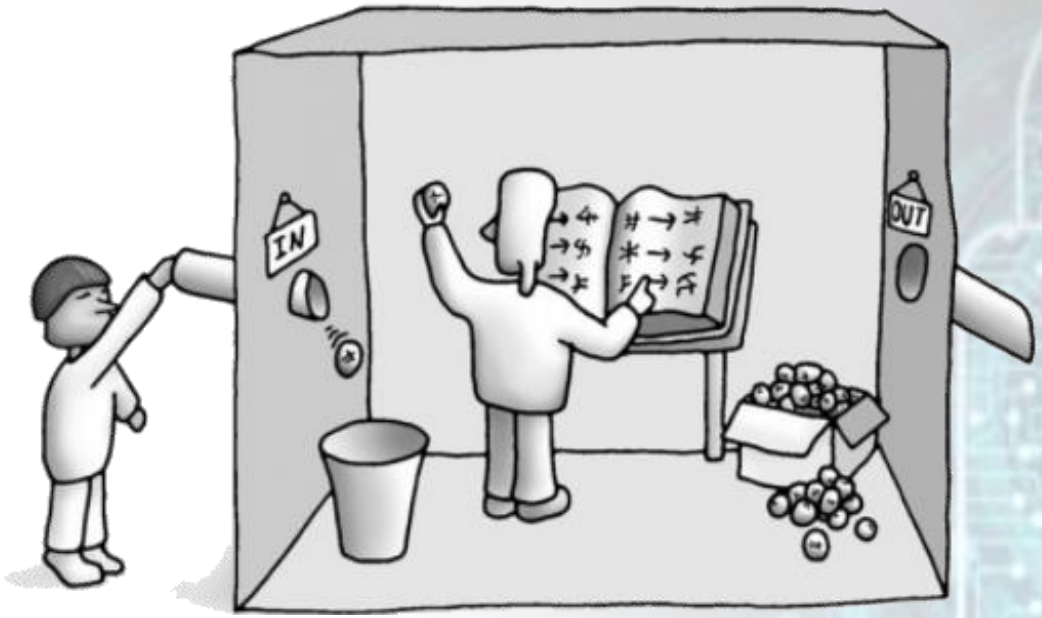
MSc. Ing. Guido Rosales

EL DESARROLLO DE SOFTWARE EN NUMEROS

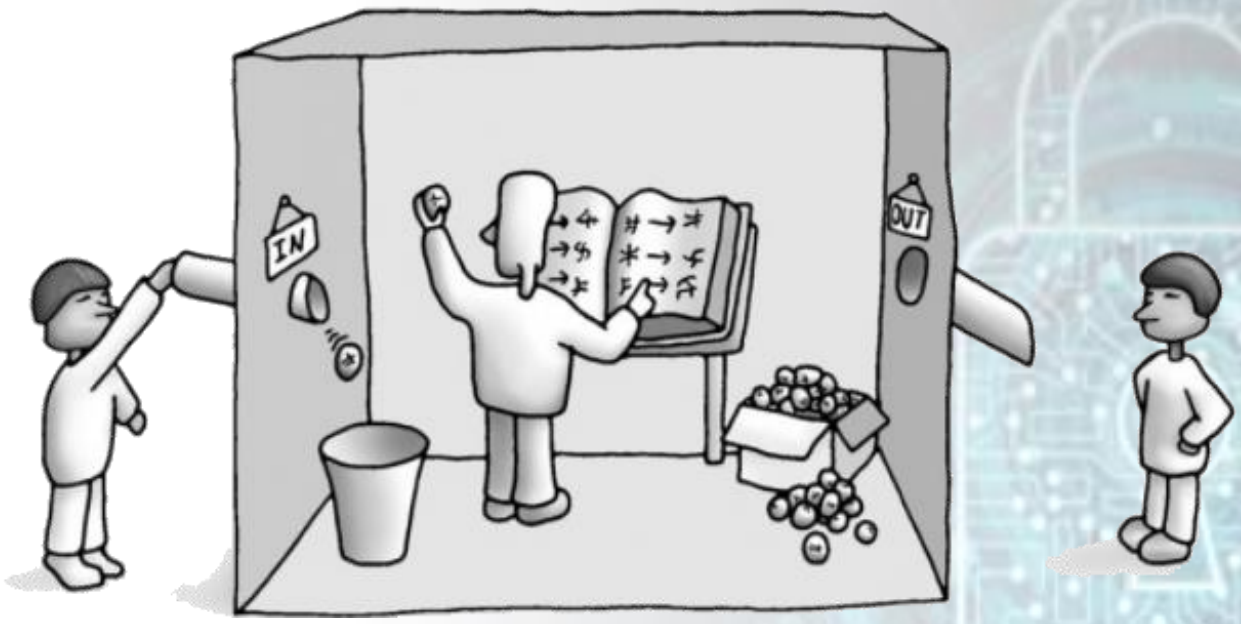
- Argentina, 4.200 empresas emplean a 81.000 personas y en 2015 obtuvieron US$ 1.004 millones en ingresos por ventas al exterior. (BID)
- Uruguay genera 16.000 empleos directos y está integrado por 470 empresas que en 2015 exportaron US$ 400 millones a más de 52 mercados (BID)
- Chile, las empresas del sector exportan U$S 370 millones y sus principales clientes son los países de América Latina y, en menor medida, Estados Unidos y Europa. (BID)
- ECUADOR a 2017 – 45 millones en exportaciones con 700 empresas (estudio elaborado por la Escuela de Negocios (Espae).
- la industria de **software** genera **ventas** del orden de **$ 500 millones** (0,5% del PIB), con un crecimiento anual de 17% en los siete años previos. La actividad más importante es la **provisión de servicios informáticos** (53%), al tiempo que las ventas de software al sector público representan 22% del total.



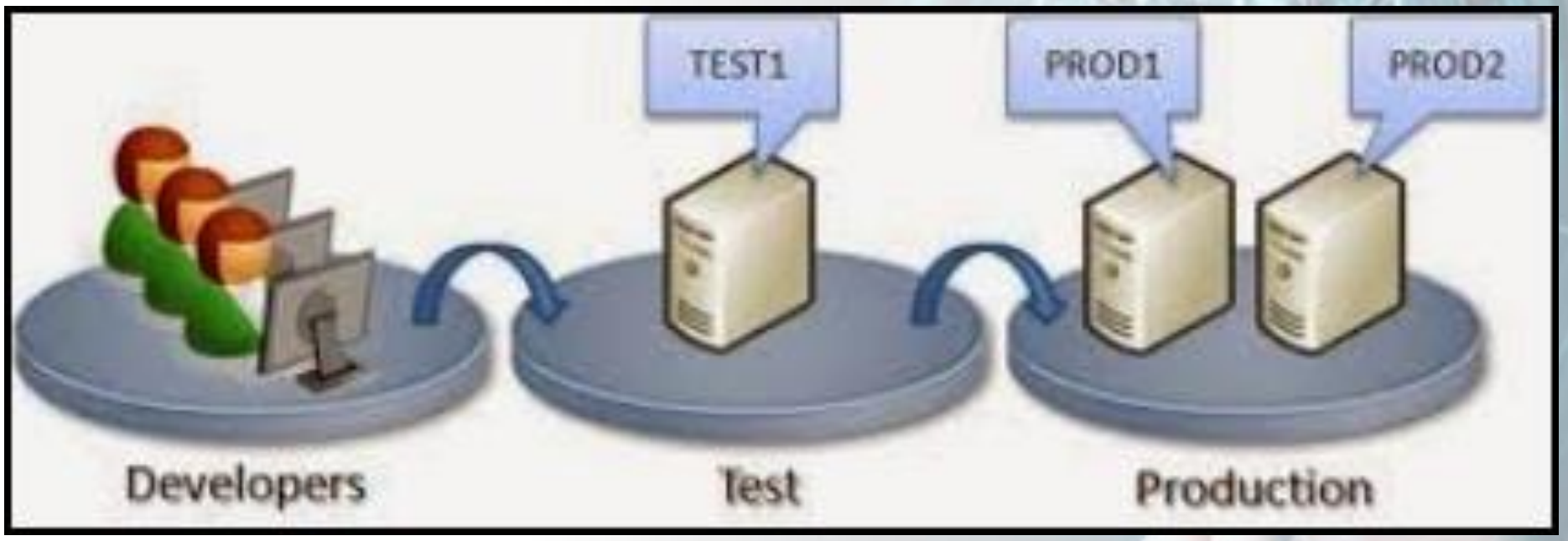
MSc. Ing. Guido Rosales


IN
OUT


CIBERCRIMINALES
6".0"
5".0"
4".0"
3".0
Hacker_
Black Hats_
Hacktivistas_
Script Kiddies_

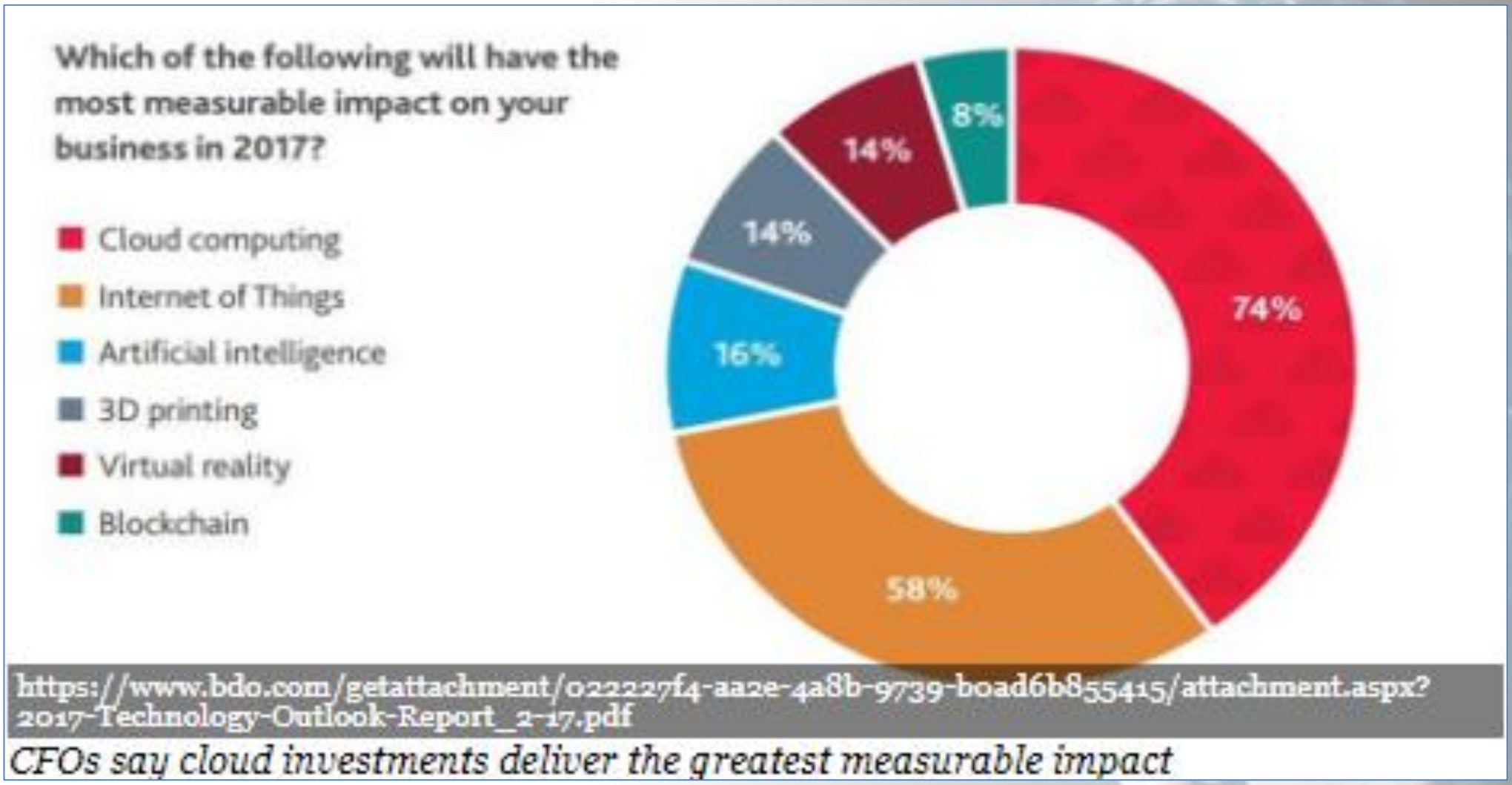

IN
OUT


CIBERCRIMINALES
6".0"
5".0"
4".0"
3".0
Hacker_
Black Hats_
Hacktivistas_
Script Kiddies_

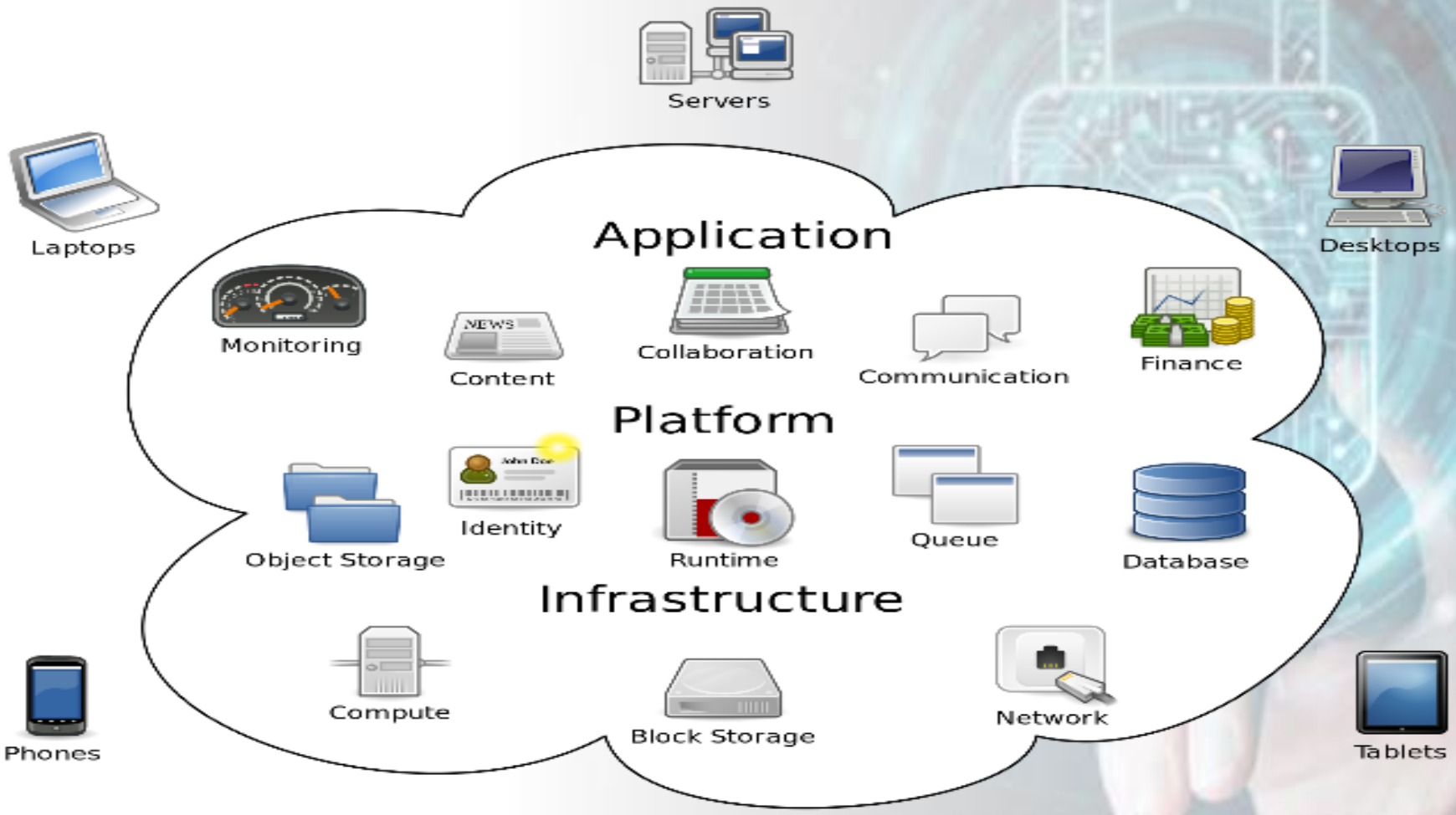

TEST1
PROD1
PROD2
Developers
Test
Production

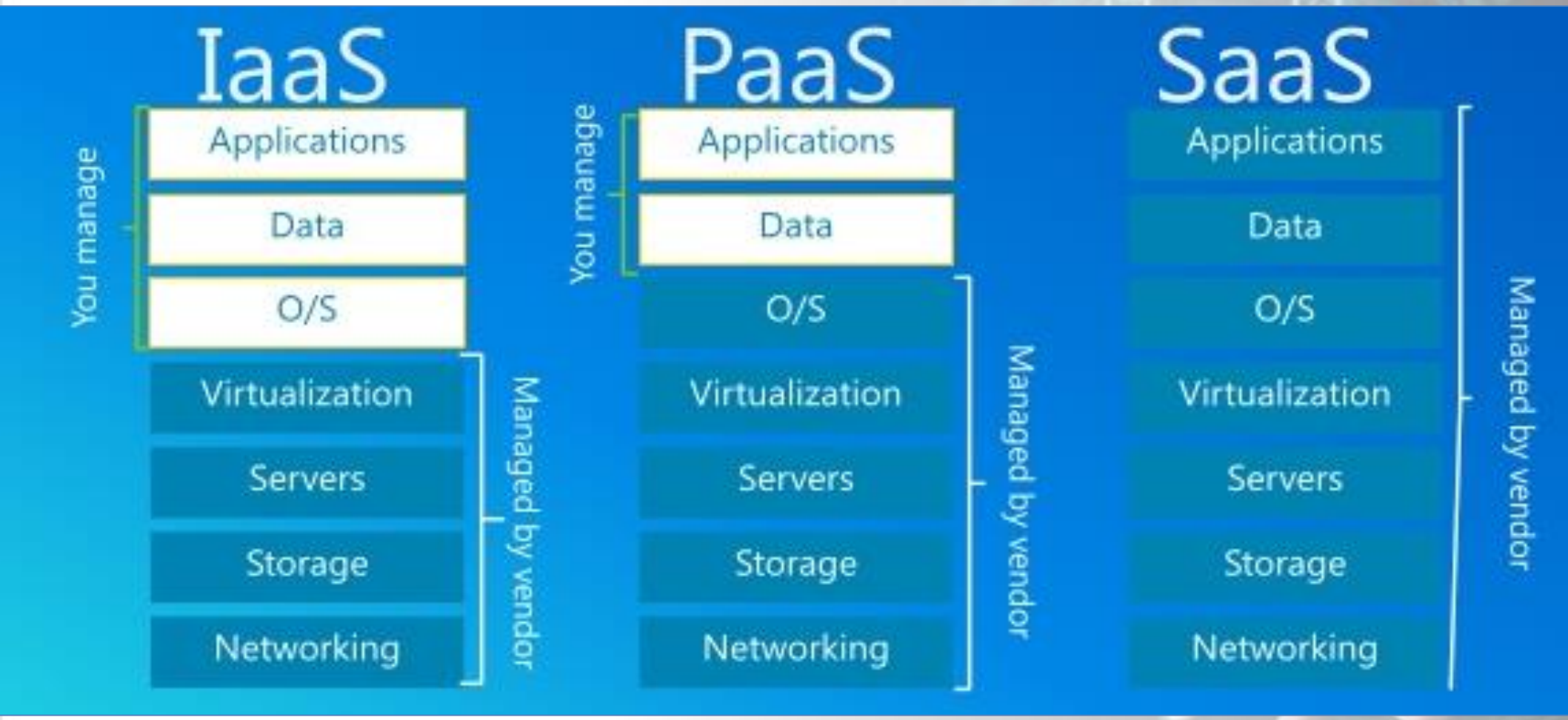
NECESITAMOS PROTEGER LAS APLICACIONES
DE QUE? DONDE? QUIEN?

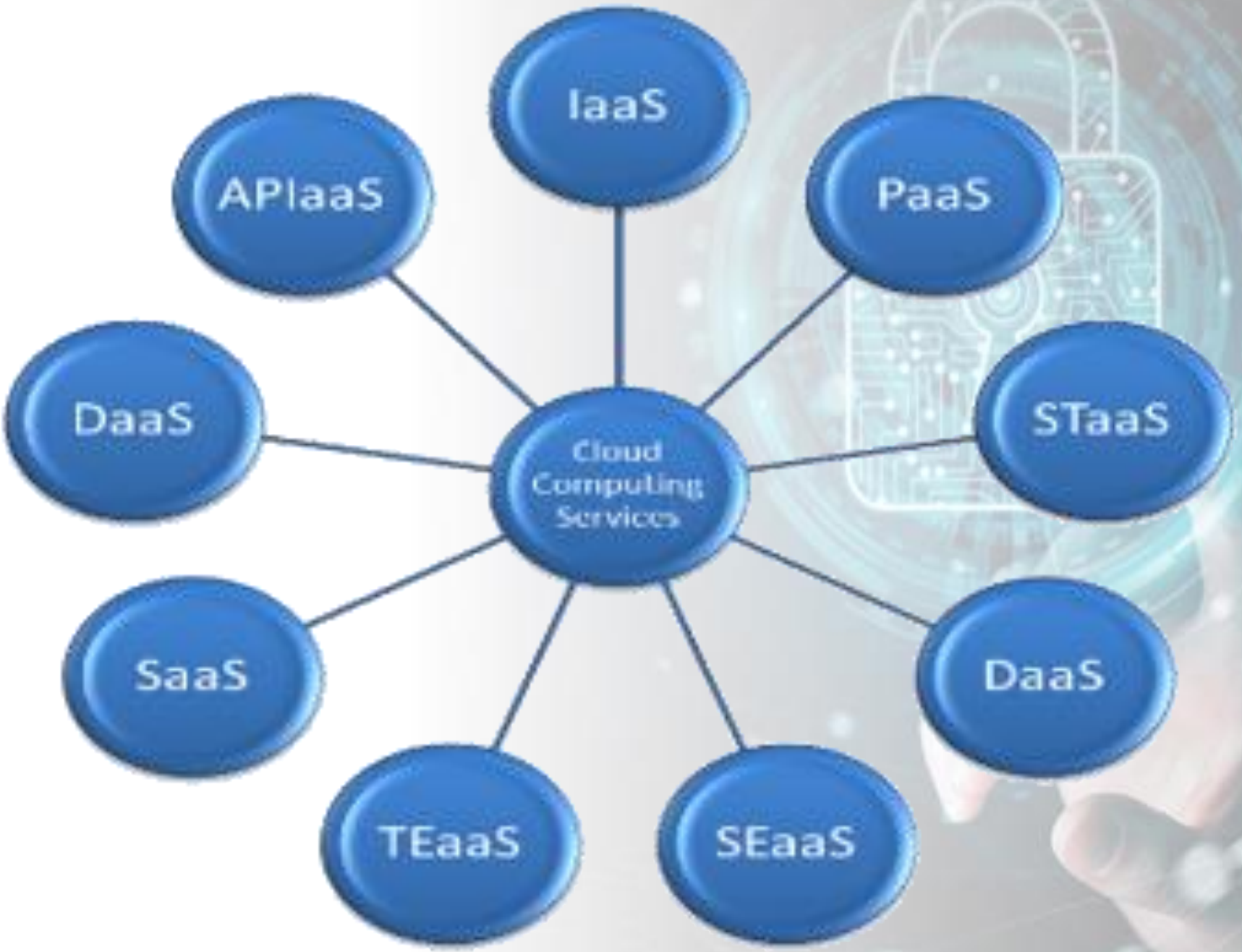
MSc. Ing. Guido Rosales



CFOs say cloud investments deliver the greatest measurable impact


Servers
Laptops
Desktops
Application
Monitoring
Content
Collaboration
Communication
Finance
Platform
Identity
Object Storage
Runtime
Queue
Database
Infrastructure
Compute
Block Storage
Network
Phones
Tablets
Cloud Computing


IaaS
Applications
Data
O/S
Virtualization
Servers
Storage
Networking
You manage
Managed by vendor
PaaS
Applications
Data
O/S
Virtualization
Servers
Storage
Networking
You manage
Managed by vendor
SaaS
Applications
Data
O/S
Virtualization
Servers
Storage
Networking
Managed by vendor



MSc. Ing. Guido Rosales

Cloud pública

→

La cloud pública pertenece y es administrada por empresas que la utilizan para ofrecer acceso rápido a recursos informáticos accesibles a otras empresas o personas individuales. Con los servicios de cloud pública, los usuarios no necesitan adquirir hardware, software o infraestructura de soporte, sino que se encargan los proveedores.

Cloud privada

→

La cloud privada pertenece y es administrada por una única empresa, que controla el modo en que las distintas líneas de negocio y grupos integrantes personalizan y utilizan los recursos virtualizados y los servicios automatizados. La cloud privada permite aprovechar muchas eficiencias de la cloud, además de proporcionar un mayor control y evitar la multitenencia.

Cloud híbrida

→

La cloud híbrida utiliza una base de cloud privada, combinada con el uso estratégico de servicios de cloud pública. En realidad, una cloud privada no puede existir aislada del resto de los recursos de TI de una empresa ni de la cloud pública. La mayoría de las empresas con clouds privadas evolucionarán para gestionar cargas de trabajo entre centros de datos, clouds privadas y clouds públicas y, por lo tanto, creando clouds híbridas.

Figure 1. Magic Quadrant for Cloud Infrastructure as a Service, Worldwide

Rosales

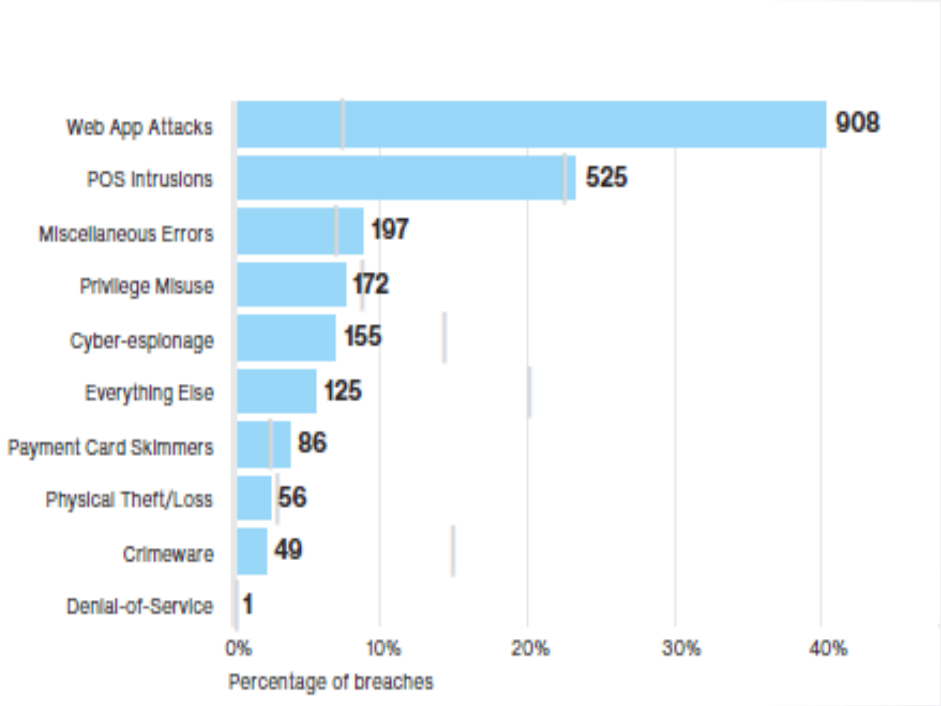
uido Rosales

Análogos	Inmigrantes Digitales	Nativos Digitales	
Baby Boombers	**Generación X**	**Generación Y**	**Generación Z**
			
(1946-1964) *Hijos de la 2° Guerra Mundial*	**(1965-1979)** *Juventud de los 80's*	**(1980-2000)** *Milennials*	**(2001-2010)** *Generación Internet*

QUIEN ES MAS JOVEN?
QUIEN ES MAS AÑEJAD@

MSc. Ing. Guido Rosales

Los ataques de aplicaciones Web representaron el 40% de todas las brechas de seguridad

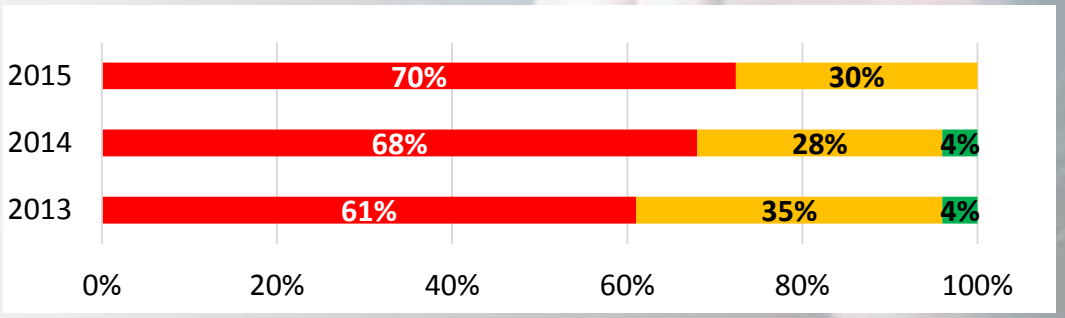


Verizon 2016 Data Breach Investigations Report

La cantidad de sitios web con vulnerabilidades de gravedad crítica está en constante crecimiento

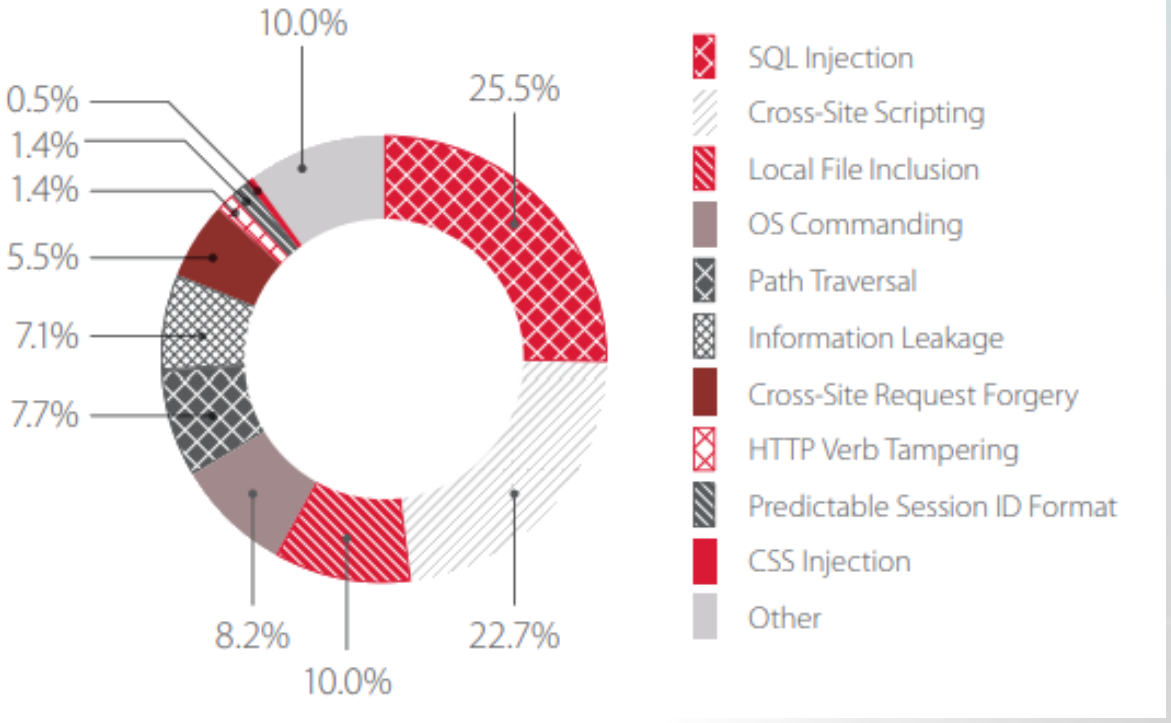
- Severidad critica
- Media
- Baja

Positive Research 2016



MSc. Ing. Guido Rosales

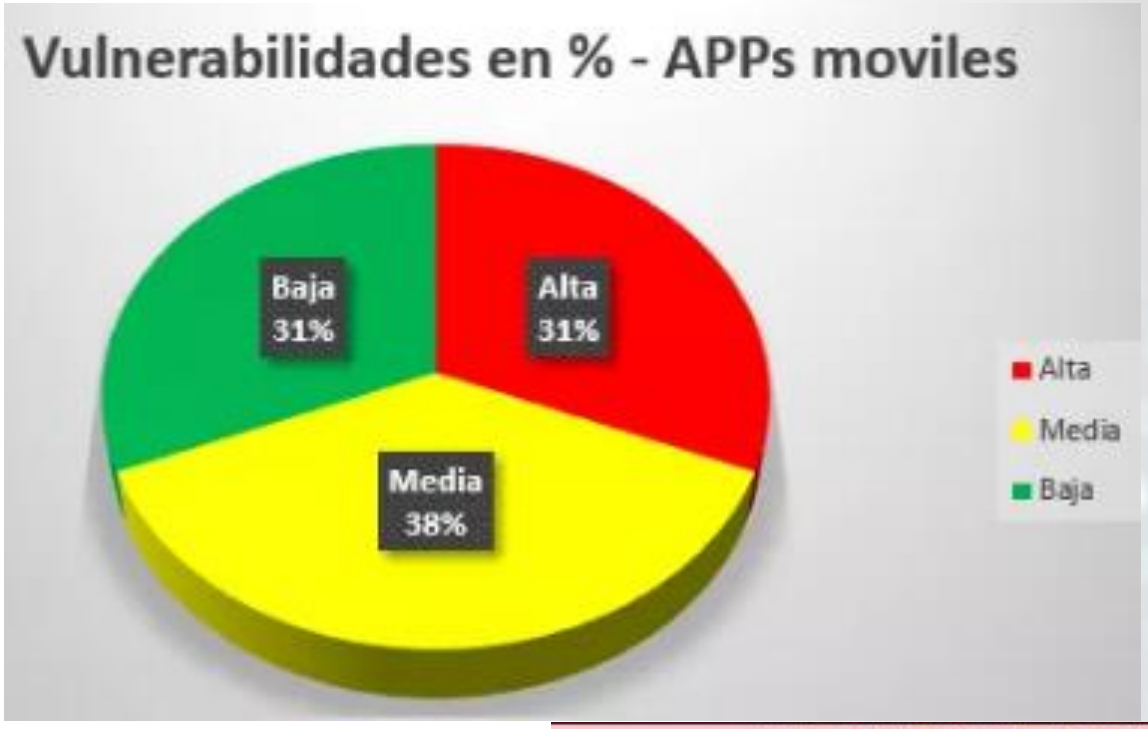
OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Inyección	→	A1:2017 – Inyección
A2 – Pérdida de Autenticación y Gestión de Sesiones	→	A2:2017 – Pérdida de Autenticación y Gestión de Sesiones
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	↘	A3:2017 – Exposición de Datos Sensibles
A4 – Referencia Directa Insegura a Objetos [Unido+A7]	∪	A4:2017 – Entidad Externa de XML (XXE) [NUEVO]
A5 – Configuración de Seguridad Incorrecta	↘	A5:2017 – Pérdida de Control de Acceso [Unido]
A6 – Exposición de Datos Sensibles	↗	A6:2017 – Configuración de Seguridad Incorrecta
A7 – Ausencia de Control de Acceso a las Funciones [Unido+A4]	∪	A7:2017 – Secuencia de Comandos en Sitios Cruzados (XSS)
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	☒	A8:2017 – Deserialización Insegura [NUEVO, Comunidad]
A9 – Uso de Componentes con Vulnerabilidades Conocidas	→	A9:2017 – Uso de Componentes con Vulnerabilidades Conocidas
A10 – Redirecciones y reenvíos no validados	☒	A10:2017 – Registro y Monitoreo Insuficientes [NUEVO, Comunidad]



MSc. Ing. Guido Rosales

UNA VISTA RÁPIDA AL DESARROLLO MOVIL

MSc. Ing. Guido Rosales



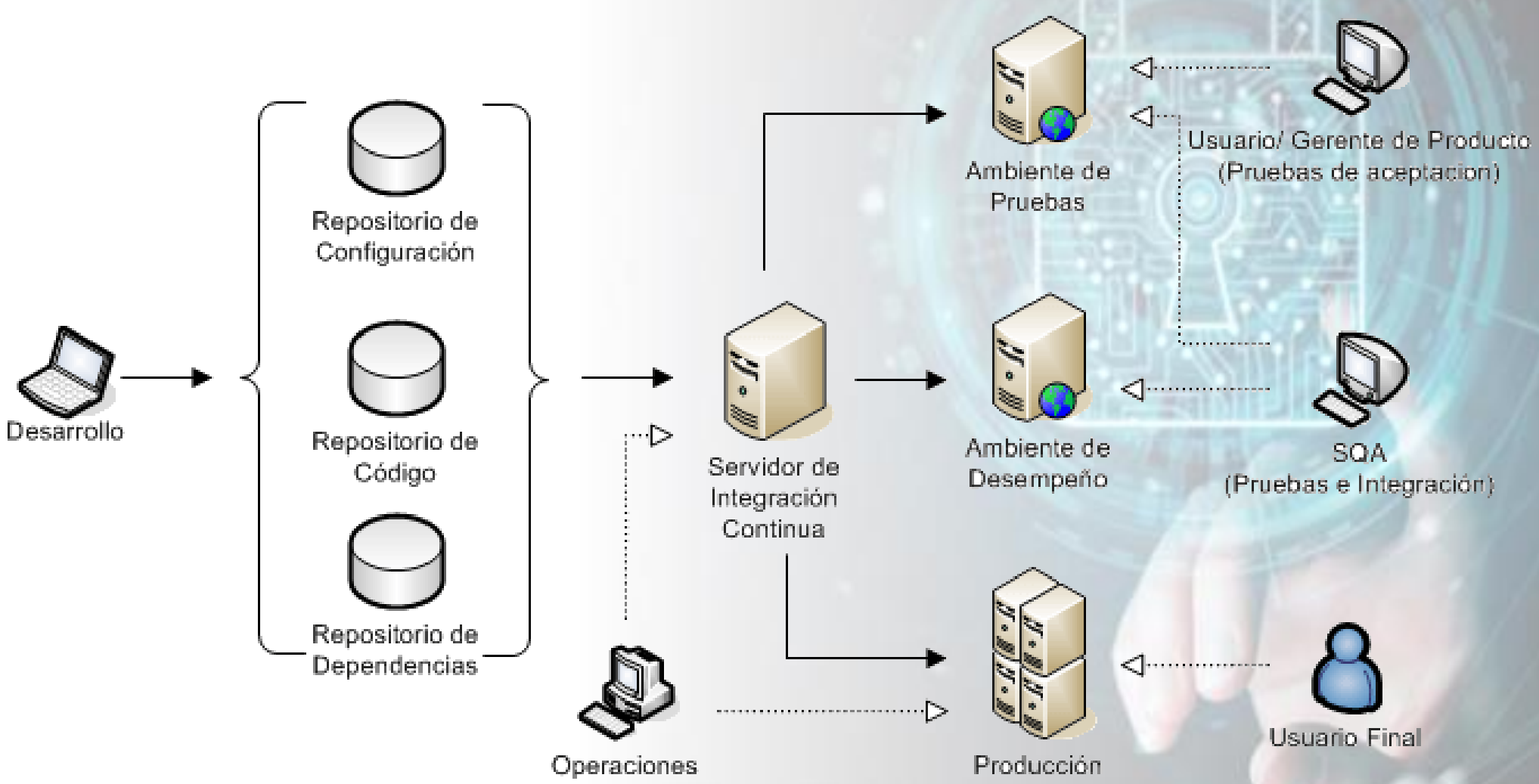
VULNERABILIDADES - Se tienen 34 Vulnerabilidades Analizadas		
Severidad	Debilidad	%
Alta	File unsafe Delete Check	55
Alta	SSL Implementation Check - SSL Certificate Verification	55
Alta	Certificate Pinning	27
Alta	Using activities/improper export of android application activities	9
Alta	Fragment Vulnerability Check	9
Media	Usage of Adb Backup	91
Media	Usage of Native codes	82
Media	Outputting Logs to logCat/ Logging Sensitive information	82
Media	SQLite Journal Information Disclosure Vulnerability	36
Media	WebView addJavascriptInterface Remote Code Execution	18
Media	Usage of Root/Superuser Permission	9
Baja	Usage of Installer verification code	91
Baja	Executing "root" or System Privilege Check	91
Baja	Emulator Detection Check	73
Baja	Unencrypted Credentials in Databases (sqlite db) Vulnerability check	18
Baja	Access Mock Location	9

Aplicación	Versión de APK	Tamaño de la APK en KB	Última Actualizacion	Version de Android
Banco Bolivariano	1.7.1	49682	27/02/2018	4.0.3
be Produbanco	1.2.0	13354	31/03/2018	1.2.0
Produbanco Grupo Promerica	2.4.0	9644	23/02/2018	2.4.0
Austro Token	1.0.0	17074	05/06/2018	4.4
Banco del Austro	1.6.5.1	7172	22/05/2018	4.1
Movilmatico (Banco del Pacifico)		3932	20/06/2018	
BGR	0.0.3	11077	15/01/2018	4.1
Banco Guayaquil	5.7.0	23122	13/06/2018	5.0
REDICHEQUE (Guayaquil)	1.0.1	6118	06/02/2018	2.2
Banca Movil (Internacional)	1.42	33299	08/03/2018	4.1
Amazonas Movil	1.0.0	1967	05/09/2017	4.0
MultiCashBG	1.0.0	21731	13/09/2017	4.1
Tus Metas BG	1.0.2	4196	25/11/2016	4.1

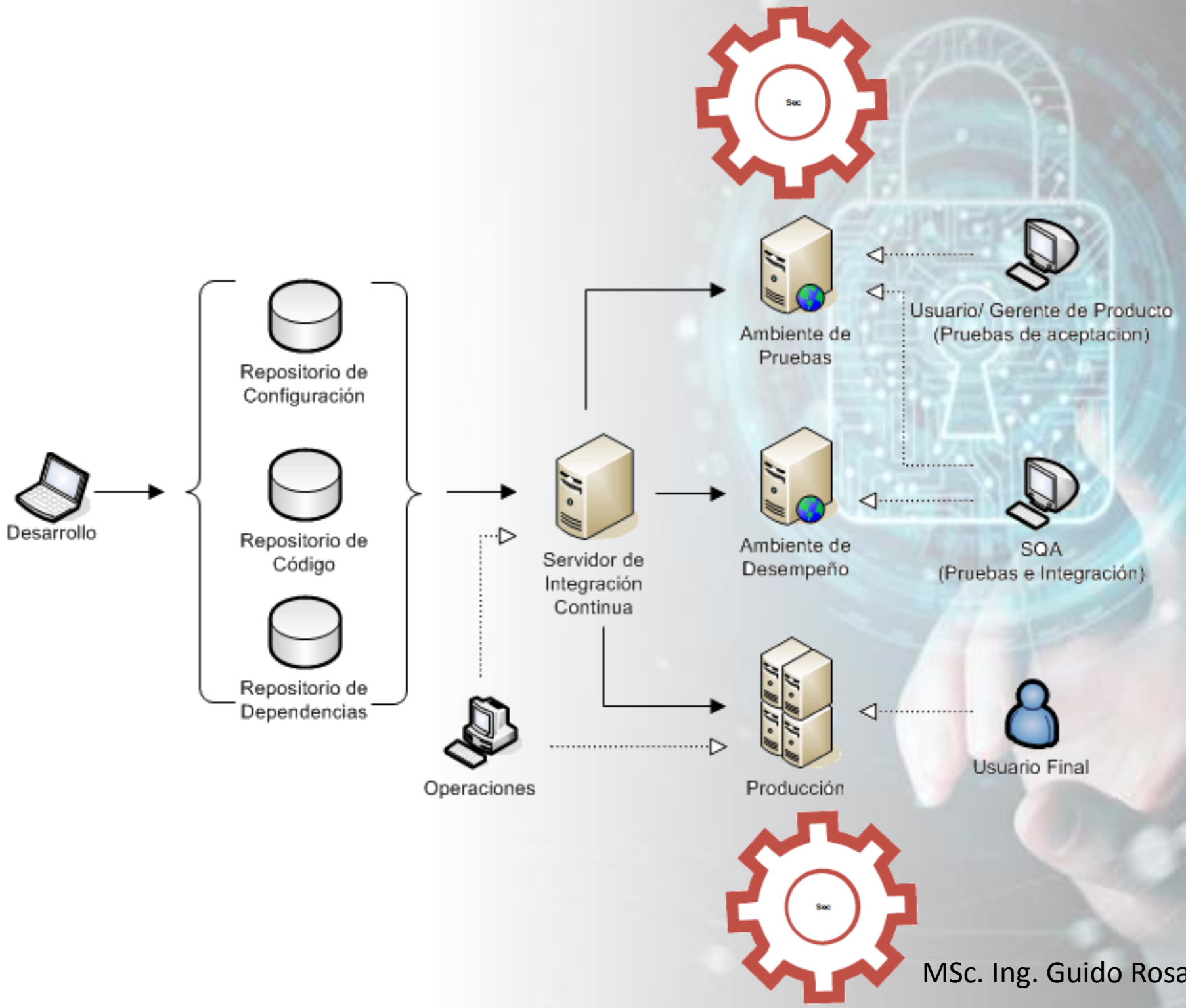
	VULNERABILIDADES - Se tienen 36 Vulnerabilidades Analizadas		
	Severidad	Debilidad	%
1	Alta	File unsafe Delete Check	76.9
2	Alta	SSL Implementation Check - SSL Certificate Verification	61.5
3	Alta	USING ACTIVITIES/IMPROPER EXPORT OF ANDROID APPLICATION ACTIVITIES	7.7
4	Alta	Certificate Pinning	0.0
5	Alta	Fragment Vulnerability Check	7.7
6	Media	WebView addJavascriptInterface Remote Code Execution	30.8
7	Media	Usage of Native codes	38.5
8	Media	Outputting Logs to logCat/ Logging Sensitive information	92.3
9	Media	Usage of Root/Superuser Permission	0.0
10	Media	Usage of Adb Backup	76.9
11	Media	SQLite Journal Information Disclosure Vulnerability	7.7
12	Media	Android PackageInfo Signature Verification / Android Fake ID Vulnerability	15.4
13	Media	Protecion of app screens by blurring when app is running in background	100.0
14	Media	Protection of capturing screenshots & sharing screens outside your app	100.0
15	Media	Protection of text fields from copying the text and paste outside your app	100.0
16	Baja	Access Mock Location	7.7
17	Baja	Usage of Installer verification code	92.3
18	Baja	Executing "root" or System Privilege Check	76.9
19	Baja	Emulator Detection Check	38.5
20	Baja	Unencrypted Credentials in Databases (sqlite db) Vulnerability check	23.1

COMO HACEMOS MAS SEGURAS LAS APLICACIONES?

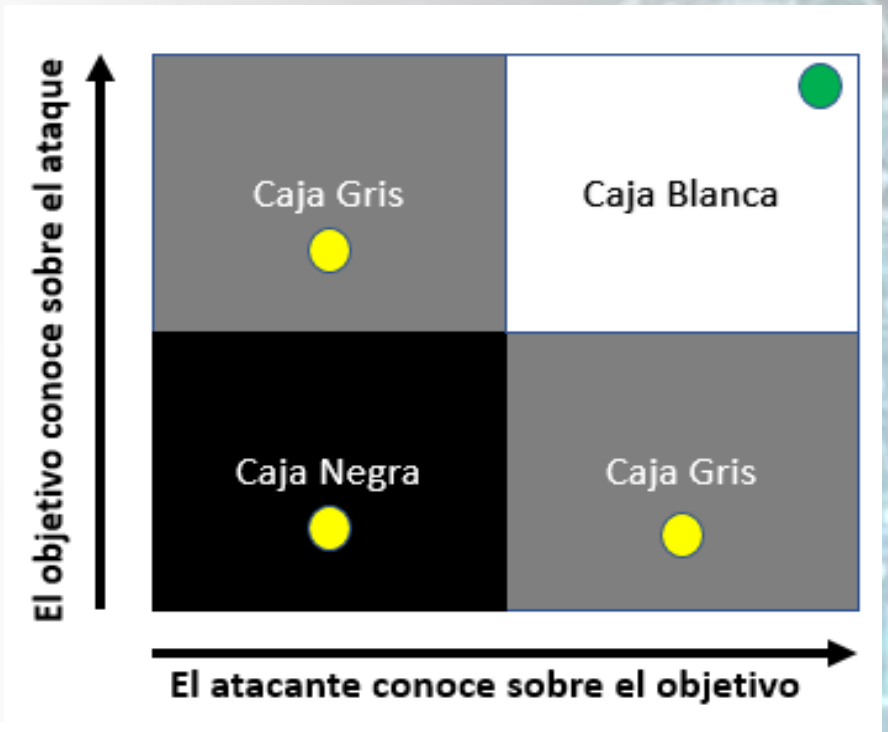
MSc. Ing. Guido Rosales

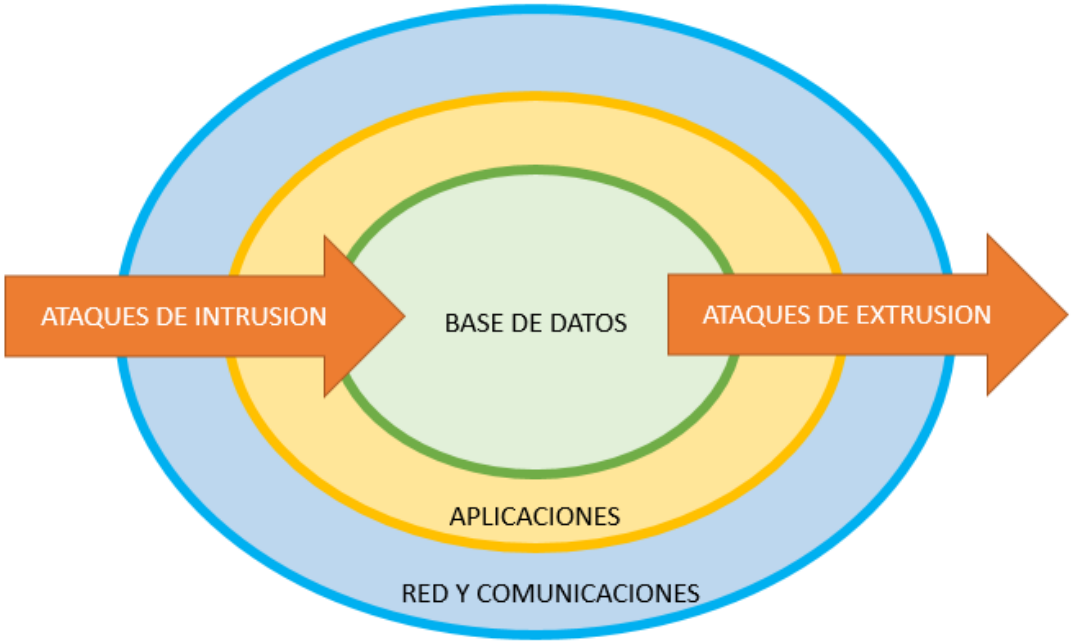


MSc. Ing. Guido Rosales



MSc. Ing. Guido Rosales

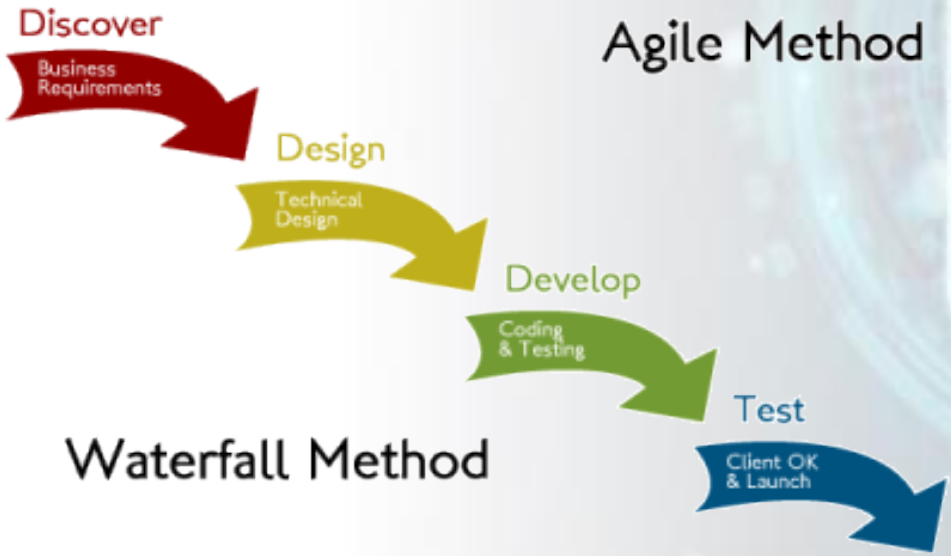




MSc. Ing. Guido Rosales

Development Methodologies

Agile Method



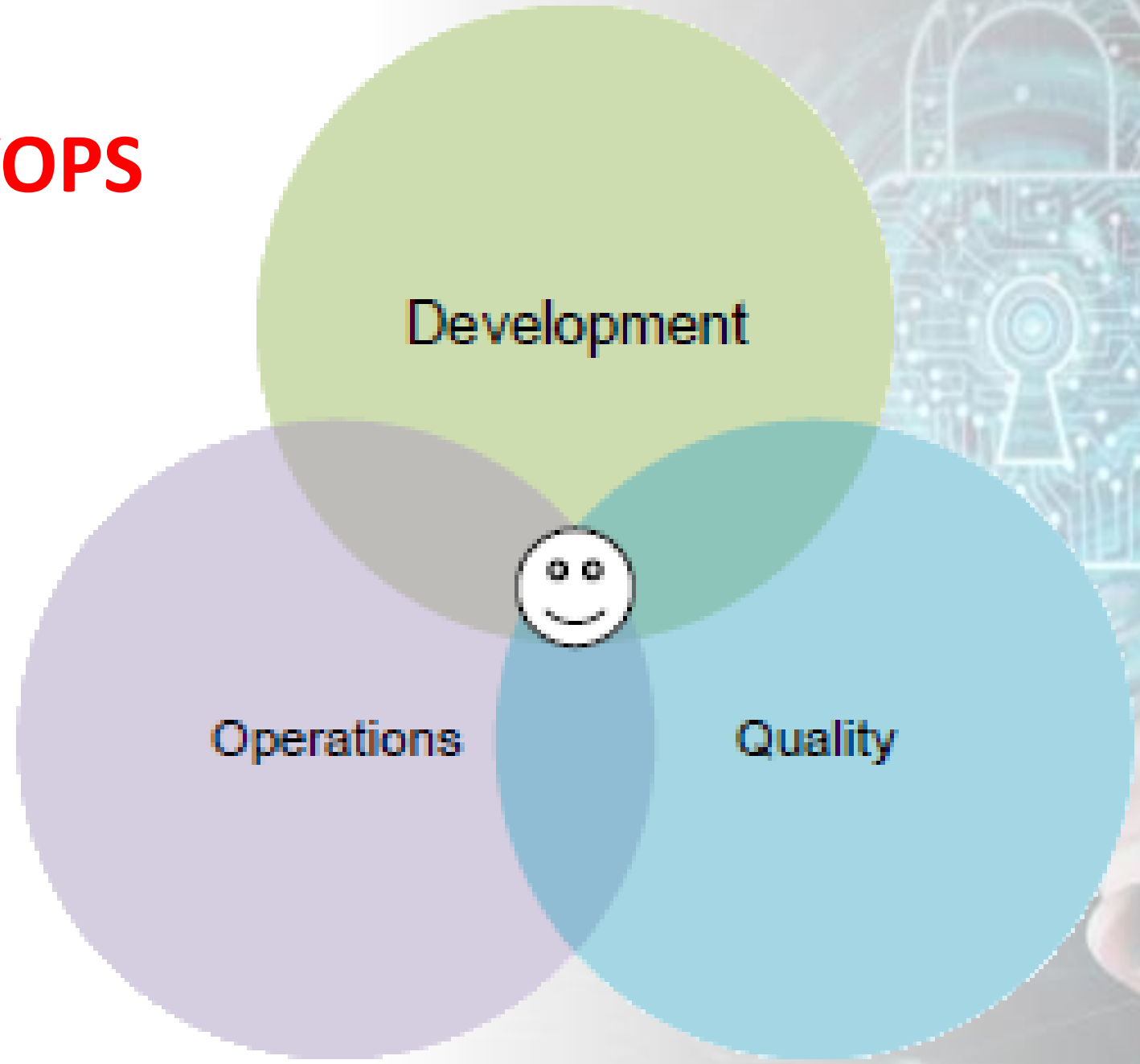
Waterfall Method

PERO..NECESITAMOS CAMBIAR?

POR QUE?....TIEMPO

MSc. Ing. Guido Rosales

DEVOPS



Project Execution Methodologies – The Change

AGILE

- Feedback from customer
- Smaller release cycles
- Focus on speed
- Not the best for business

DEVOPS

- Feedback from self
- Smaller release cycles, immediate feedback
- Focus on speed & automation
- Best for business

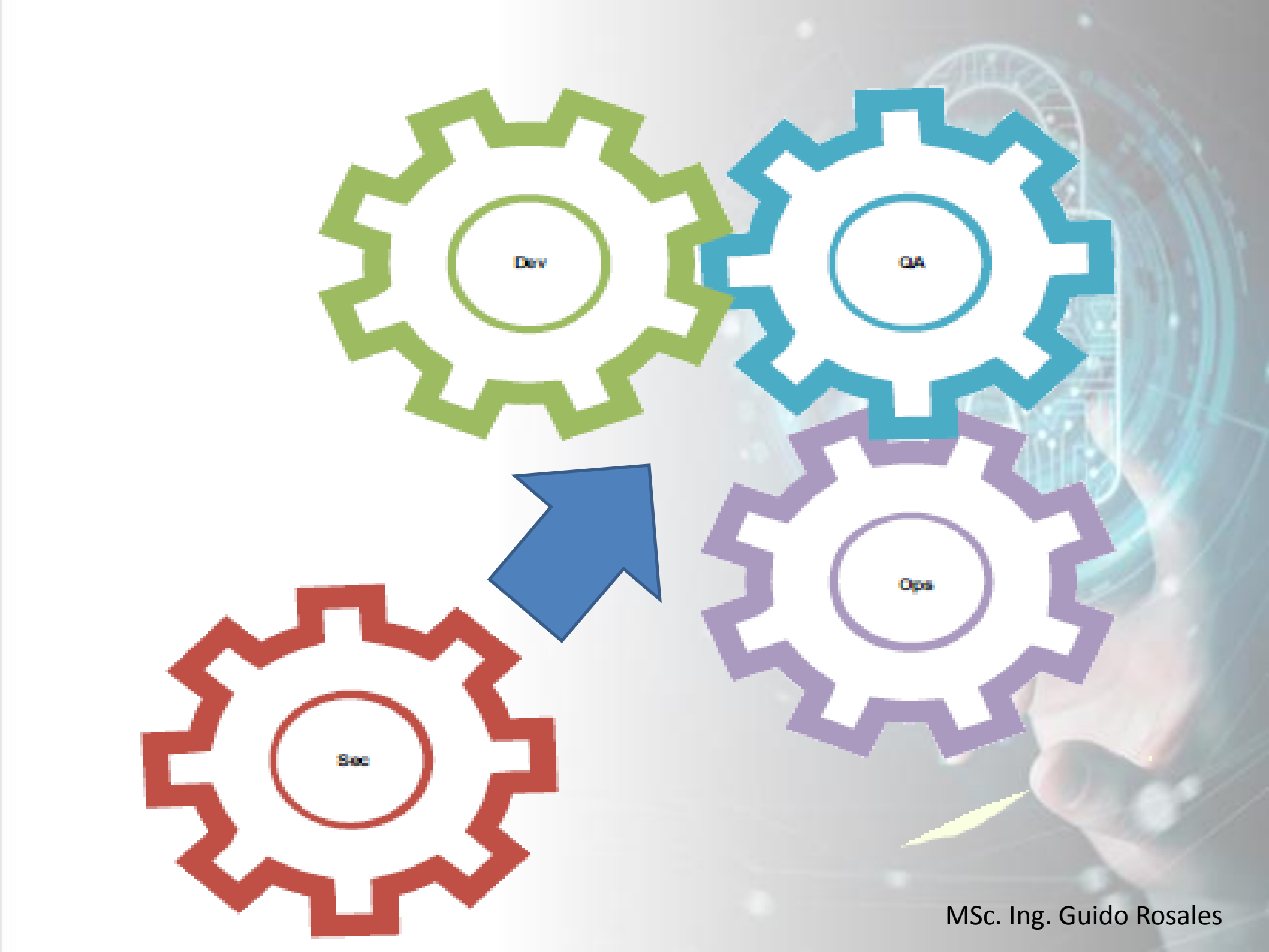
MSc. Ing. Guido Rosales

Company	Deploy Frequency	Deploy Lead Time	Reliability	Customer Responsiveness
Amazon	23,000/day	Minutes	High	High
Google	5,500/day	Minutes	High	High
Netflix	500/day	Minutes	High	High
Facebook	1/day	Hours	High	High
Twitter	3/week	Hours	High	High
Most Enterprises	Once every 9 months	Months or Quarters	Low/Med	Low/Med

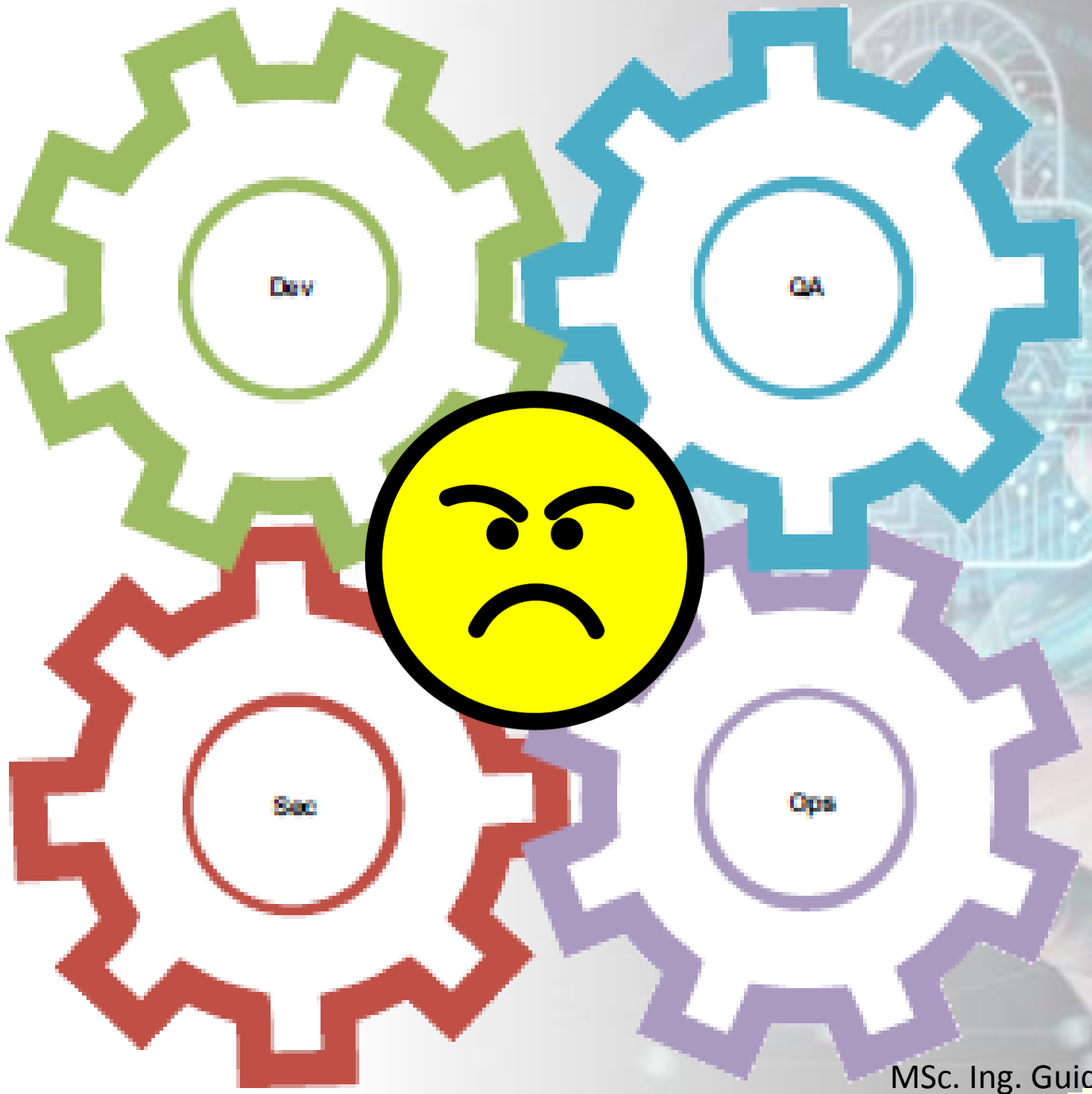
FRECUENCIA DE DESPLIEGUE

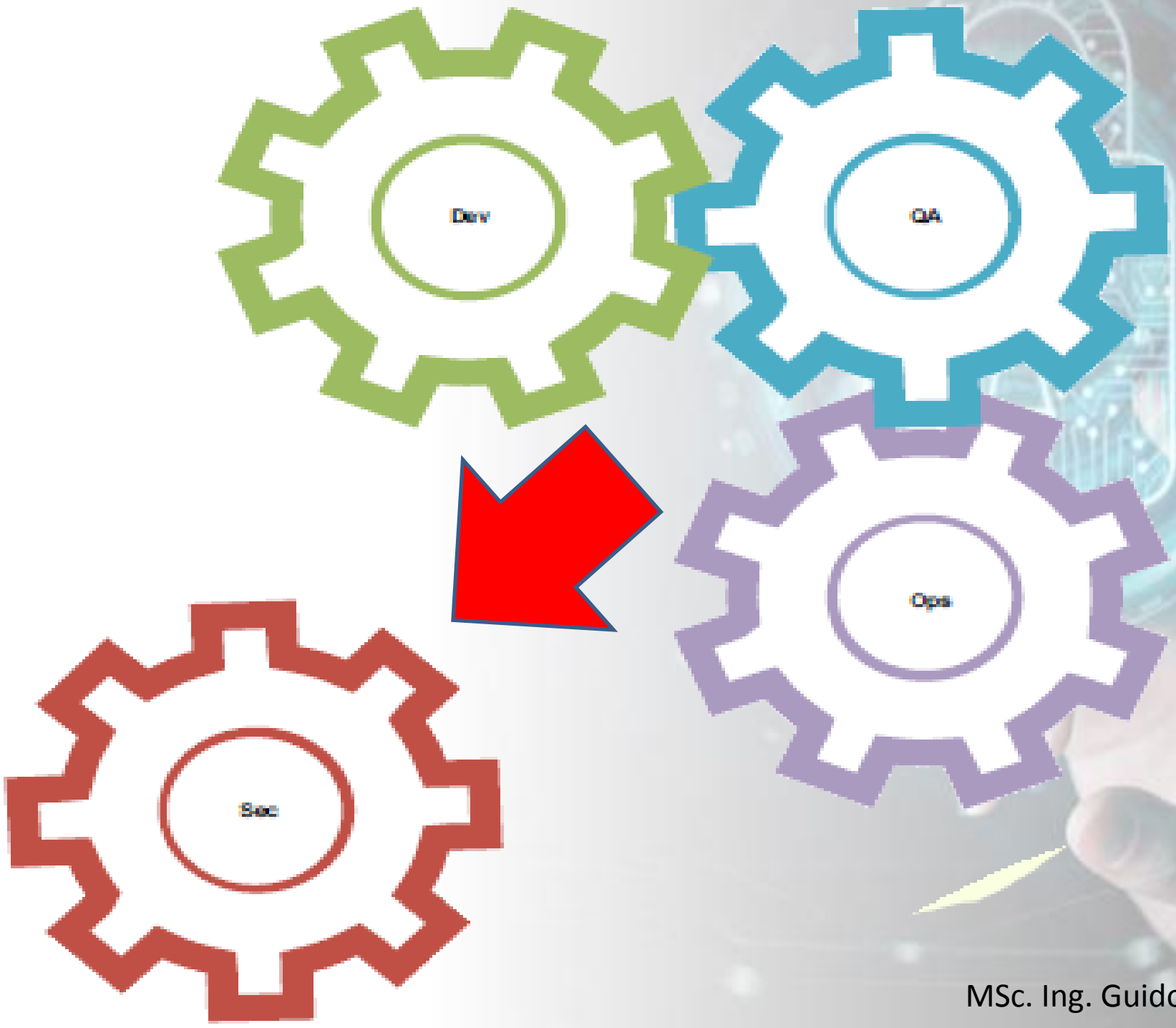
Ya somos rápidos!!...
y somos Seguros?

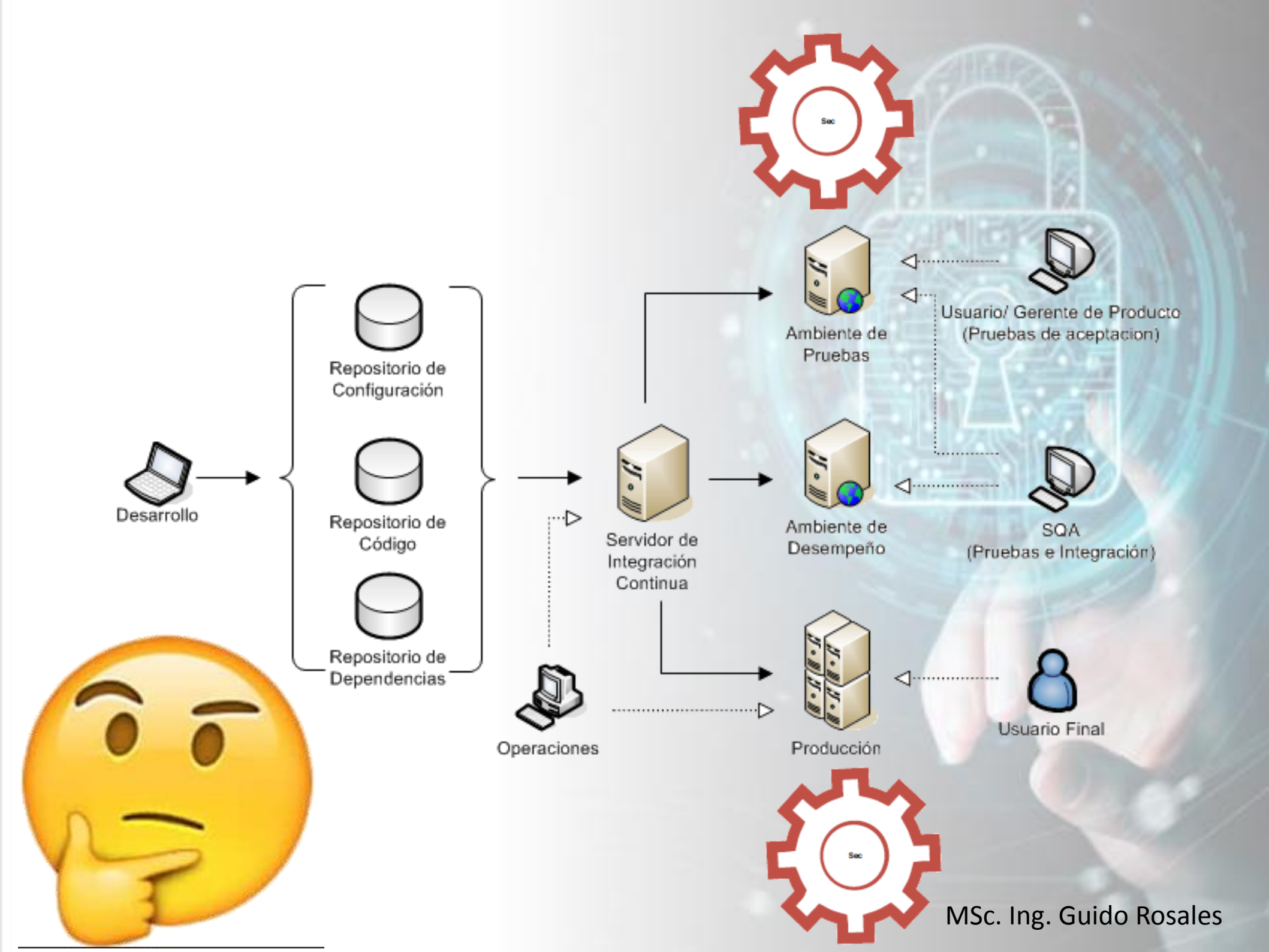
MSc. Ing. Guido Rosales

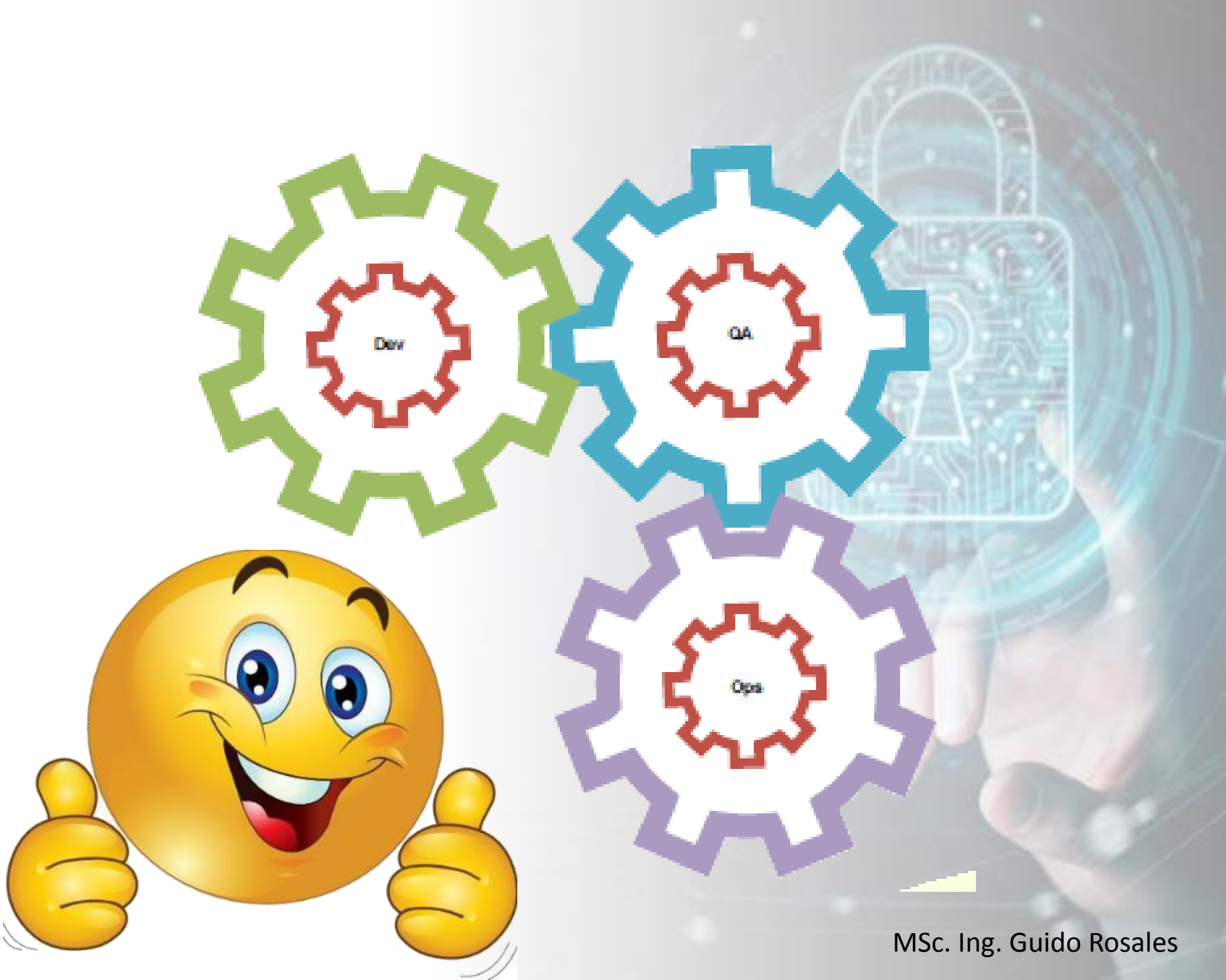


MSc. Ing. Guido Rosales

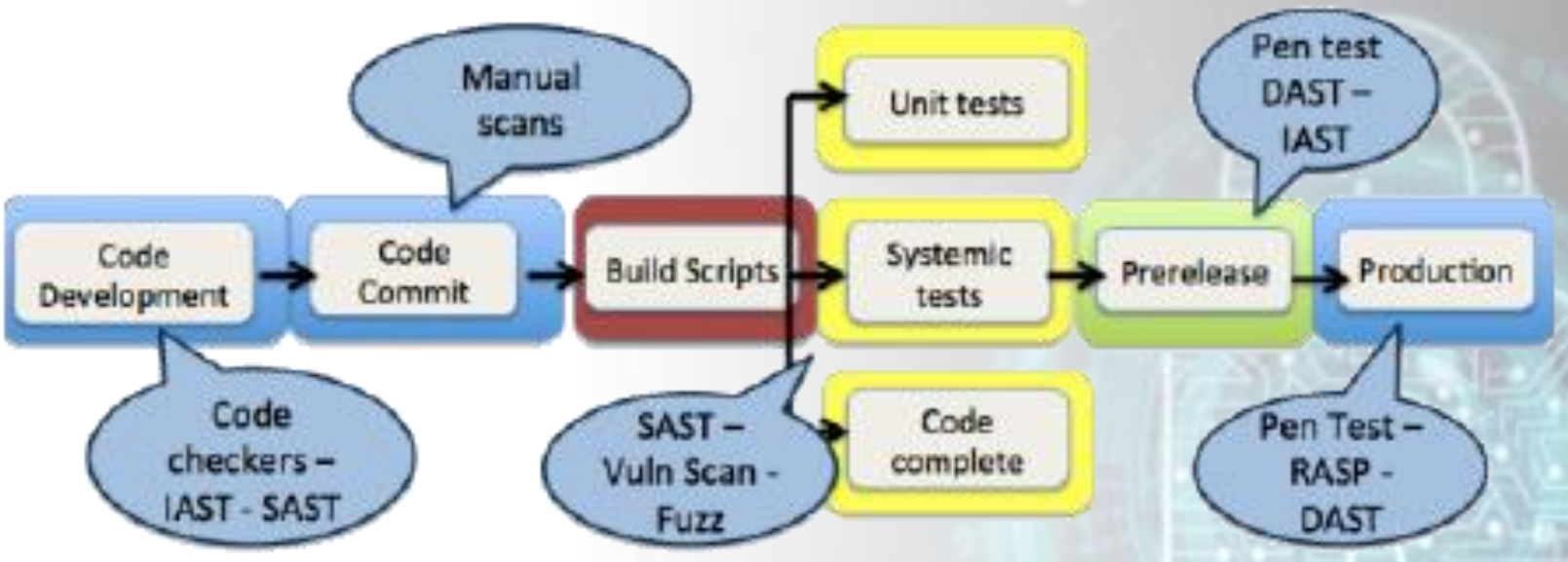

Dev
QA
Sec
Ops

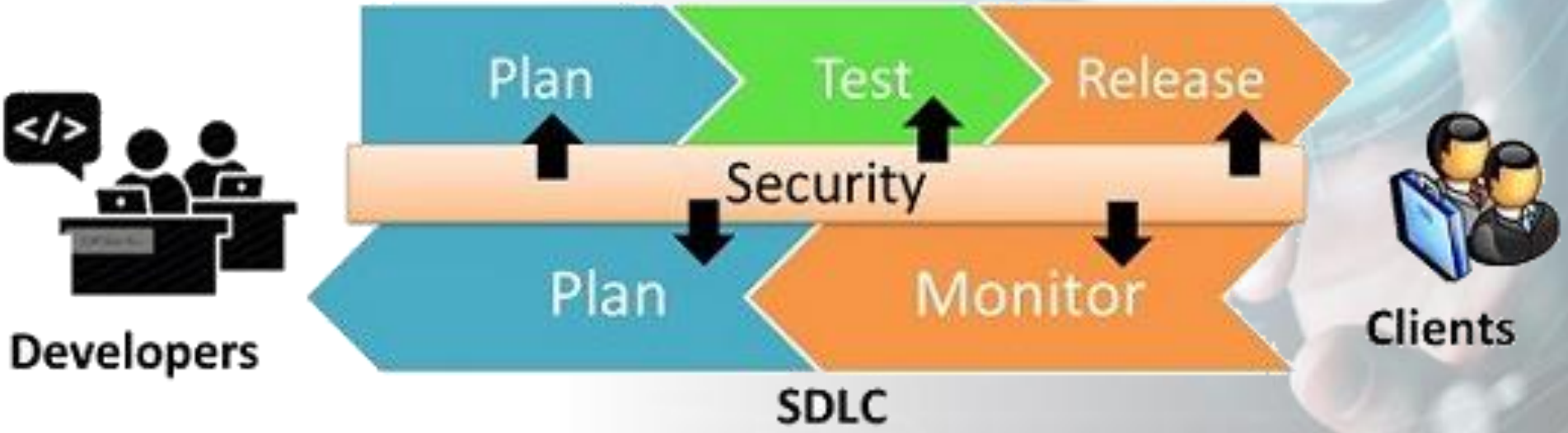

Dev
QA
Ops
Sec

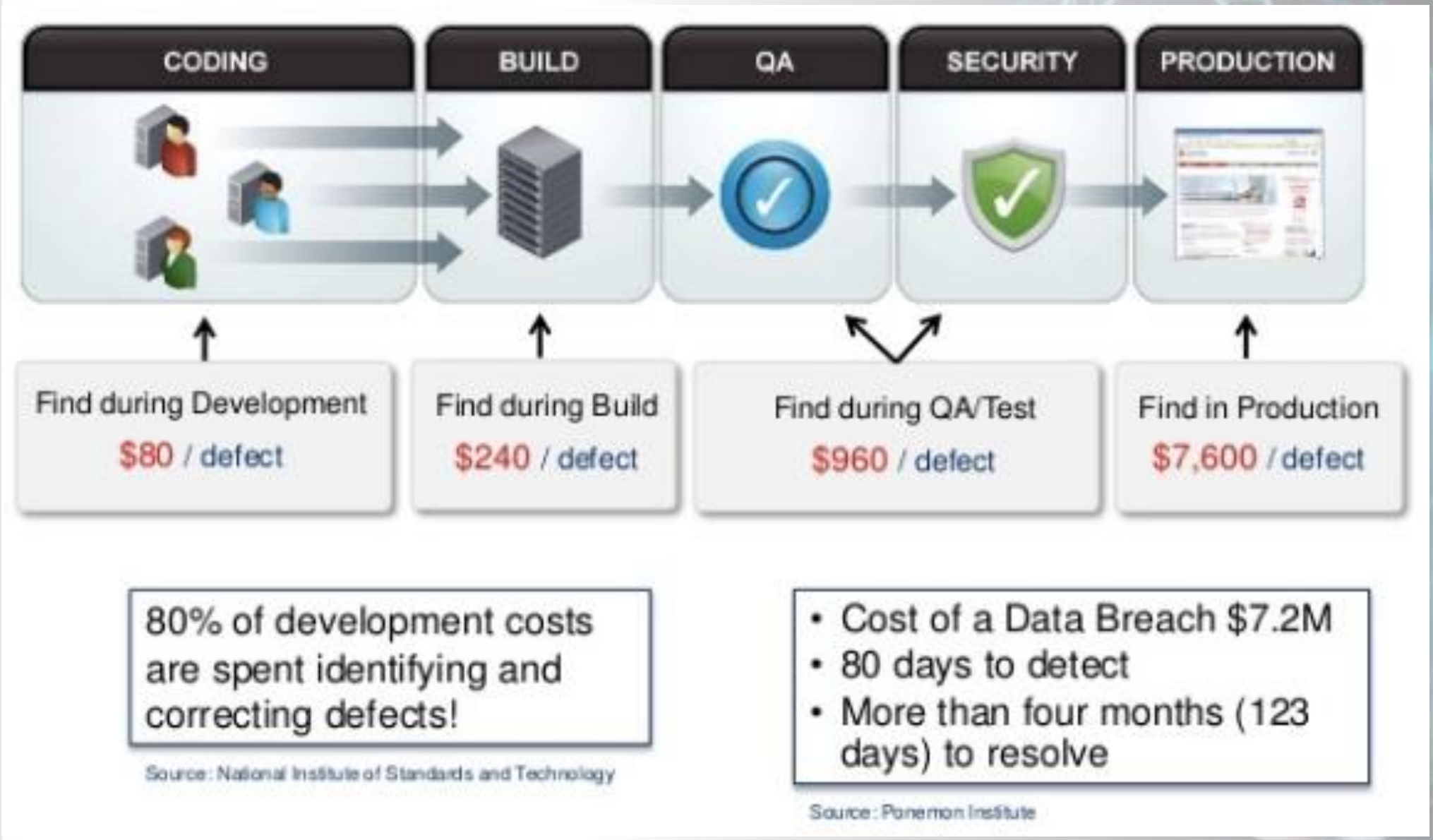

Sec
Ambiente de Pruebas
Usuario/ Gerente de Producto (Pruebas de aceptacion)
Repositorio de Configuración
Repositorio de Código
Repositorio de Dependencias
Desarrollo
Servidor de Integración Continua
Ambiente de Desempeño
SQA (Pruebas e Integración)
Operaciones
Producción
Usuario Final
Sec

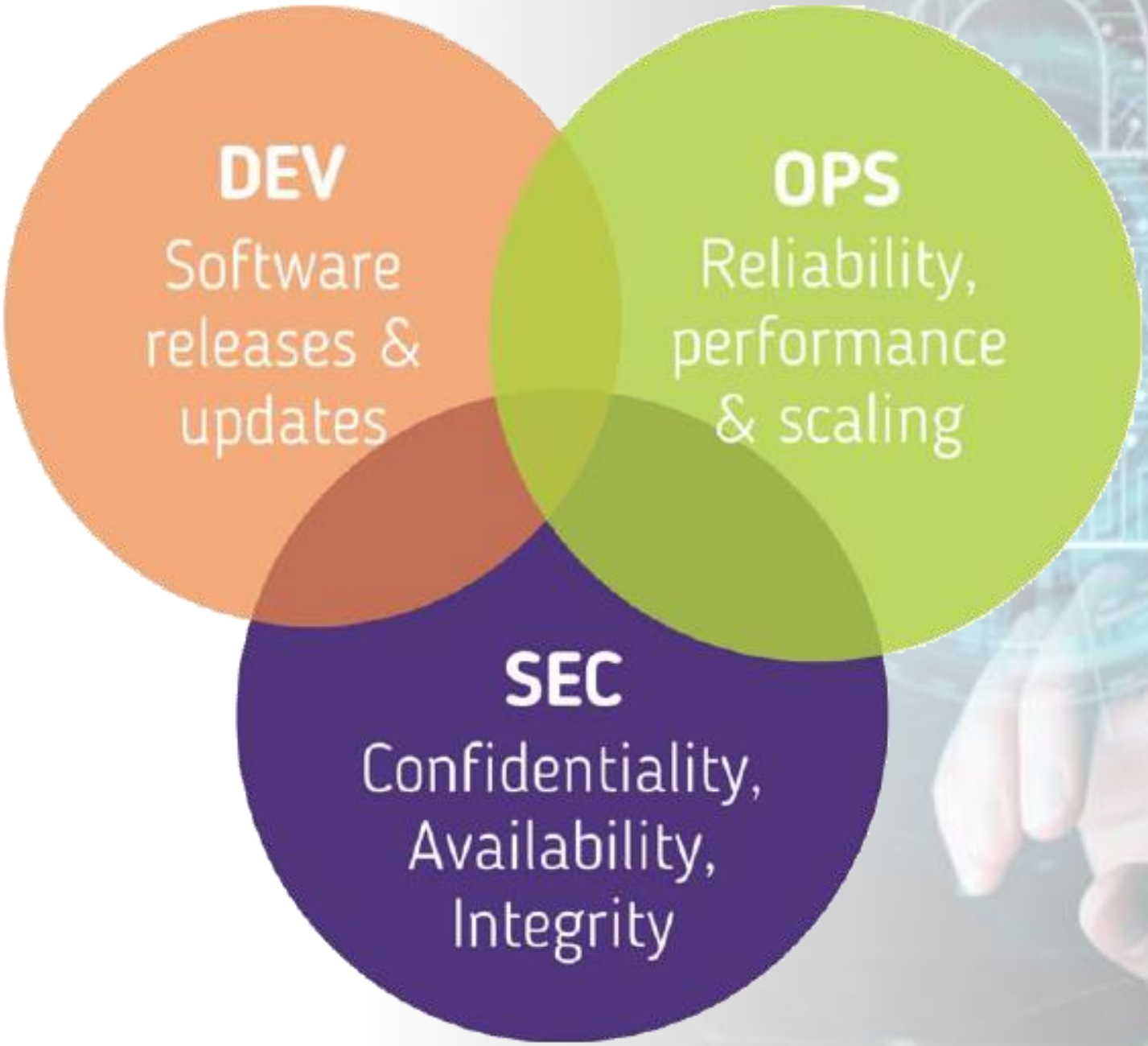


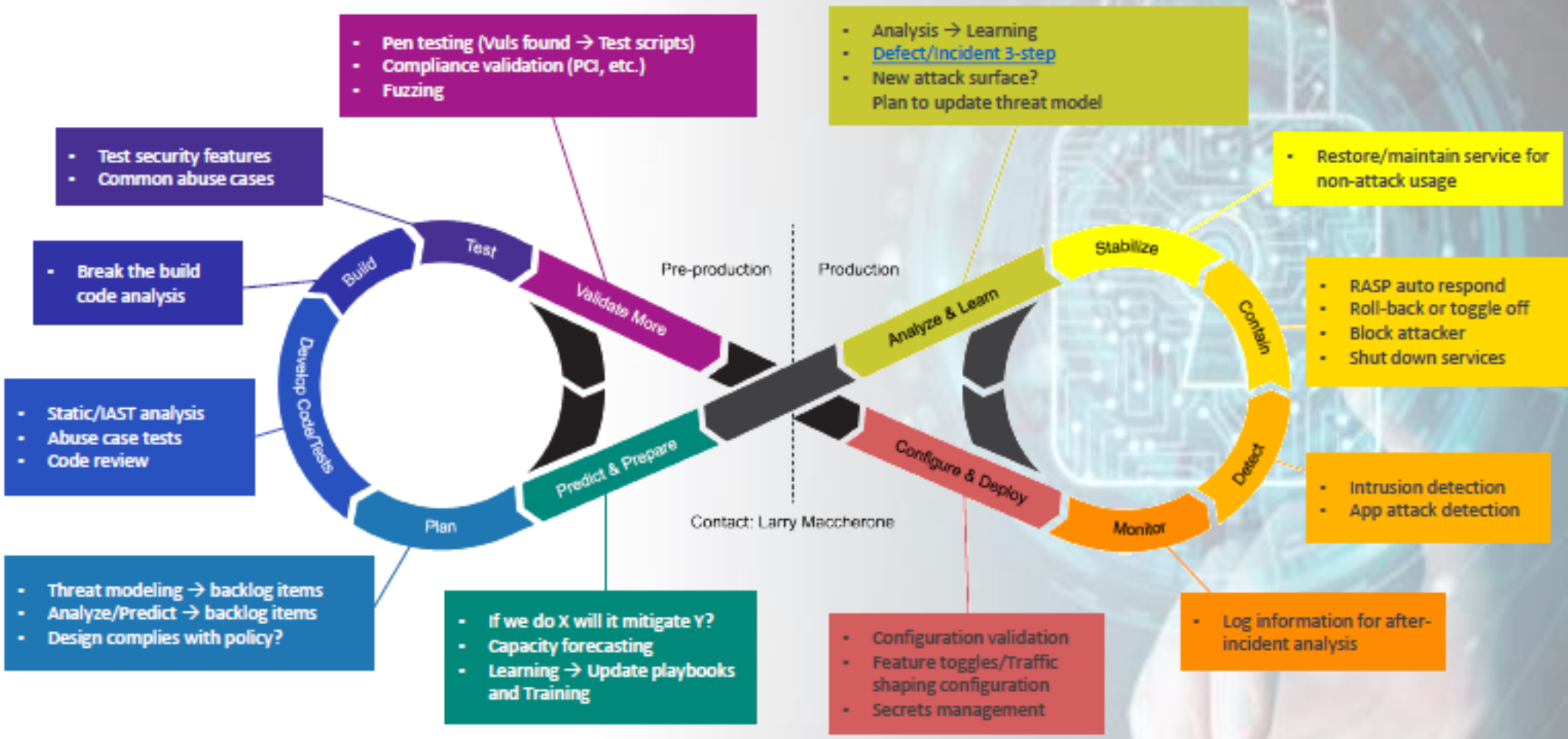
MSc. Ing. Guido Rosales


Manual scans
Unit tests
Pen test DAST – IAST
Code Development
Code Commit
Build Scripts
Systemic tests
Prerelease
Production
Code checkers – IAST - SAST
SAST – Vuln Scan - Fuzz
Code complete
Pen Test – RASP - DAST

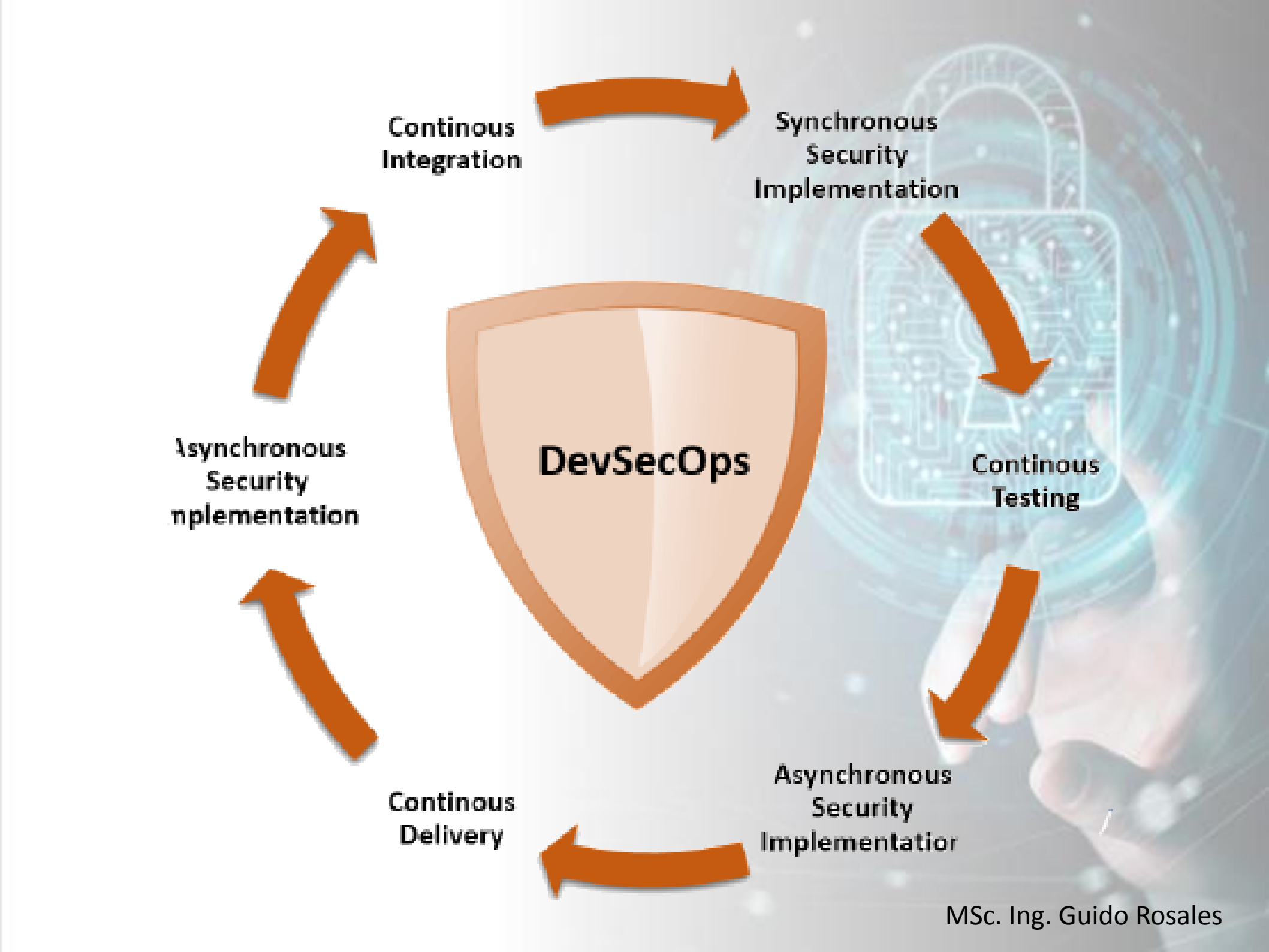

Plan
Test
Release
Security
Plan
Monitor
Developers
Clients
SDLC


CODING
BUILD
QA
SECURITY
PRODUCTION
Find during Development
$80 / defect
Find during Build
$240 / defect
Find during QA/Test
$960 / defect
Find in Production
$7,600 / defect
80% of development costs are spent identifying and correcting defects!
Source: National Institute of Standards and Technology
• Cost of a Data Breach $7.2M
• 80 days to detect
• More than four months (123 days) to resolve
Source: Ponemon Institute

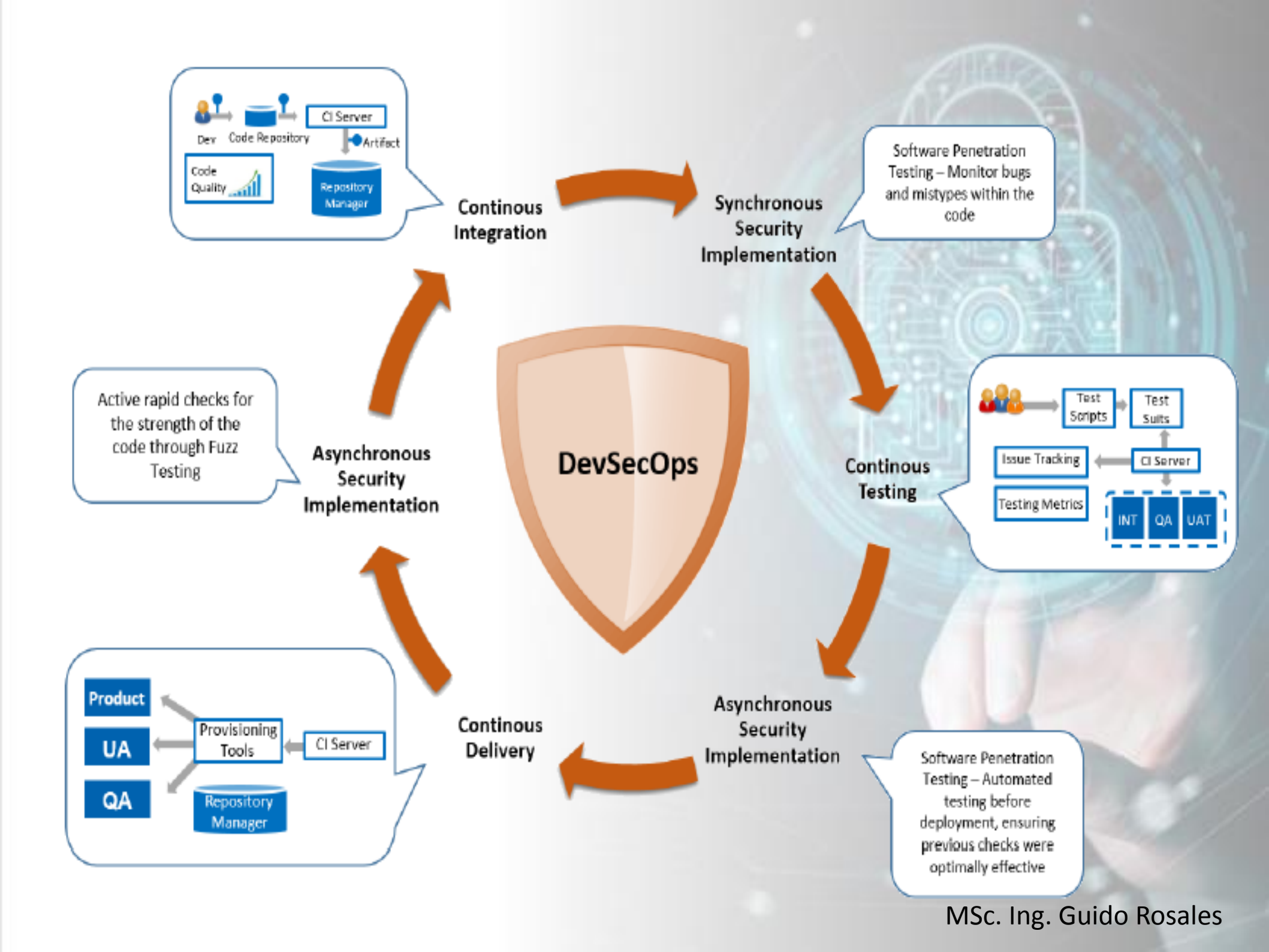

DEV
Software releases & updates
OPS
Reliability, performance & scaling
SEC
Confidentiality, Availability, Integrity



MSc. Ing. Guido Rosales



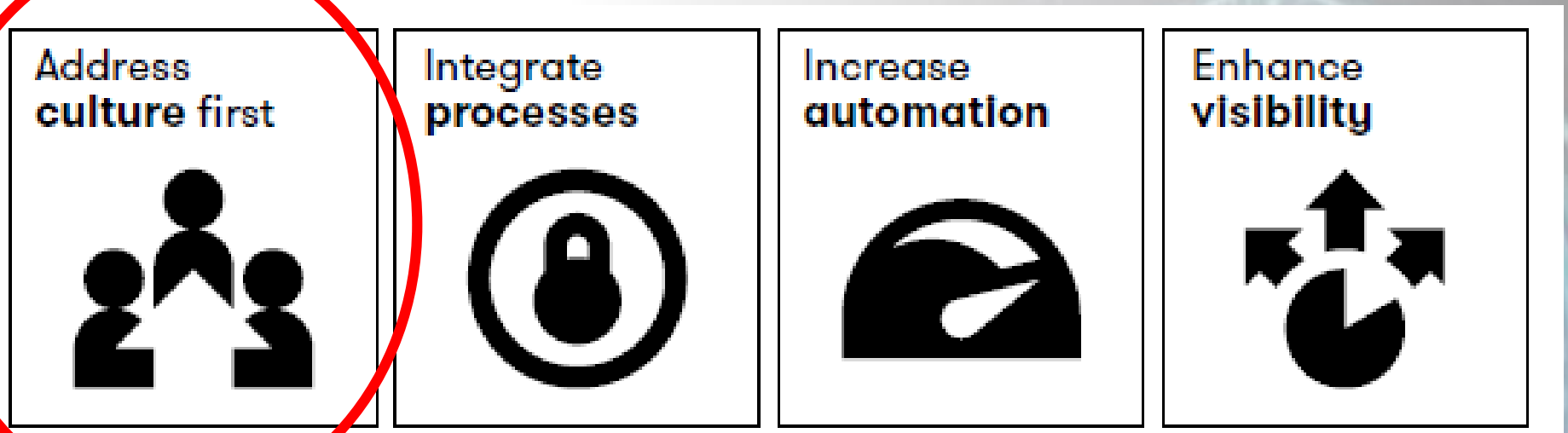
MSc. Ing. Guido Rosales



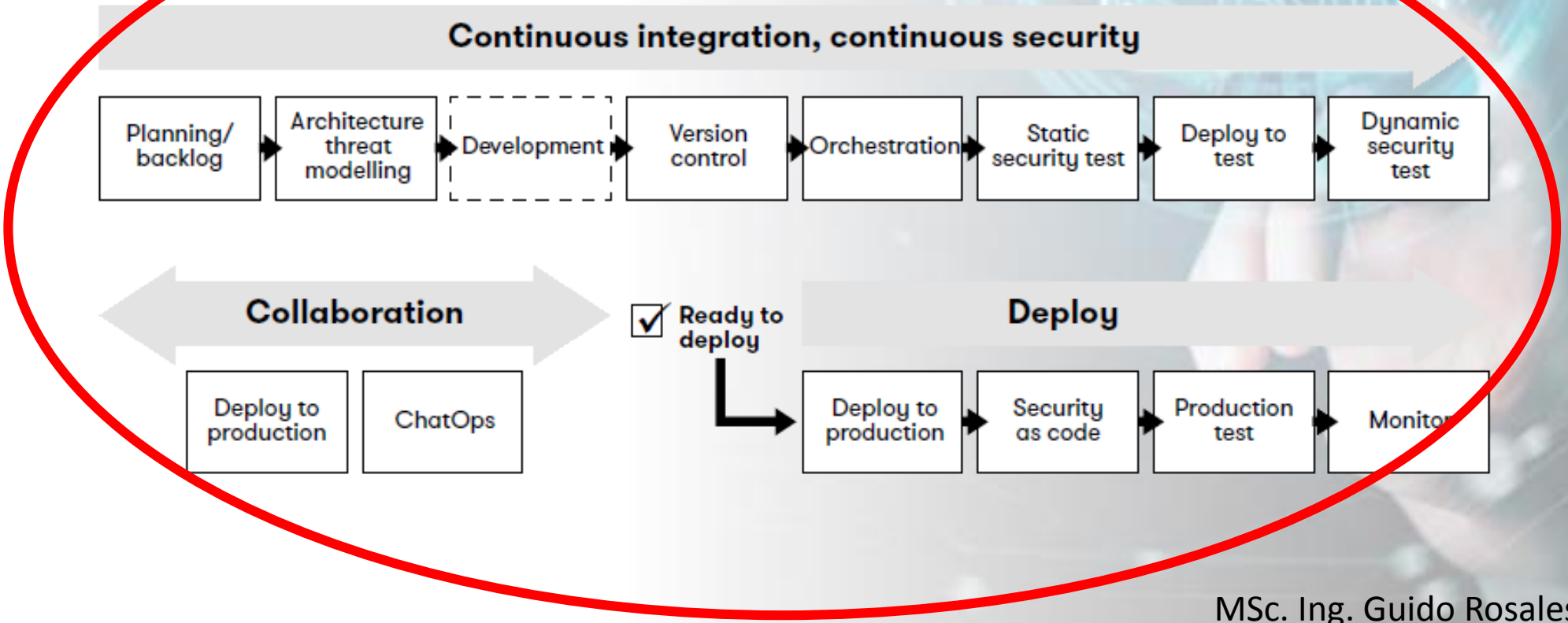
MSc. Ing. Guido Rosales

COMO IMPLEMENTAR DEVSECOPS

MSc. Ing. Guido Rosales



MSc. Ing. Guido Rosales



MSc. Ing. Guido Rosales

NETFLIX

MSc. Ing. Guido Rosales

NETFLIX

Netflix se lanzó en 1998. Al principio solamente era un servicio para alquilar DVDs a través del servicio postal de los Estados Unidos, pero Netflix sabía que el futuro estaba en la reproducción de vídeos en streaming a la carta

MSc. Ing. Guido Rosales

- 190 países de cobertura. 120 millones de usuarios
- 145 millones de horas de visualización al día
- Docenas de Tbytes x segundo
- Del 2008 al 2016 migración total a la nube
- El 2001 comenzaron con su propio CDN . Red d eentrega de contenidos
- 3000 millones $US por trimestre
- 37% del pico de trafico internet en USA
- USA dos tipos de NUBE: AWS y Open Conect

Ubicaciones de los proveedores de servicios de Internet Punto de intercambio de Internet (el tamaño de los círculos refleja el volumen)

MSc. Ing. Guido Rosales

NETFLIX

- Chaos Monkey
- Chaos Gorilla
- Chaos Kong
- Janitor Monkey
- Doctor Monkey
- Compliance Monkey
- Latency Monkey
- Security Monkey

Chaos Monkey is a resiliency tool that helps applications tolerate random instance failures.

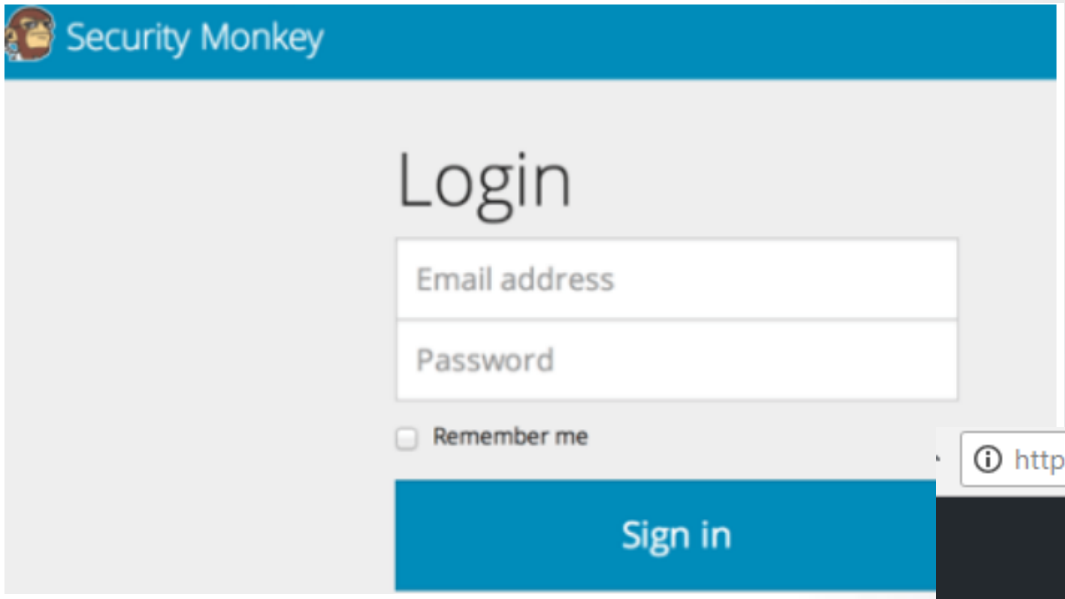
NETFLIX

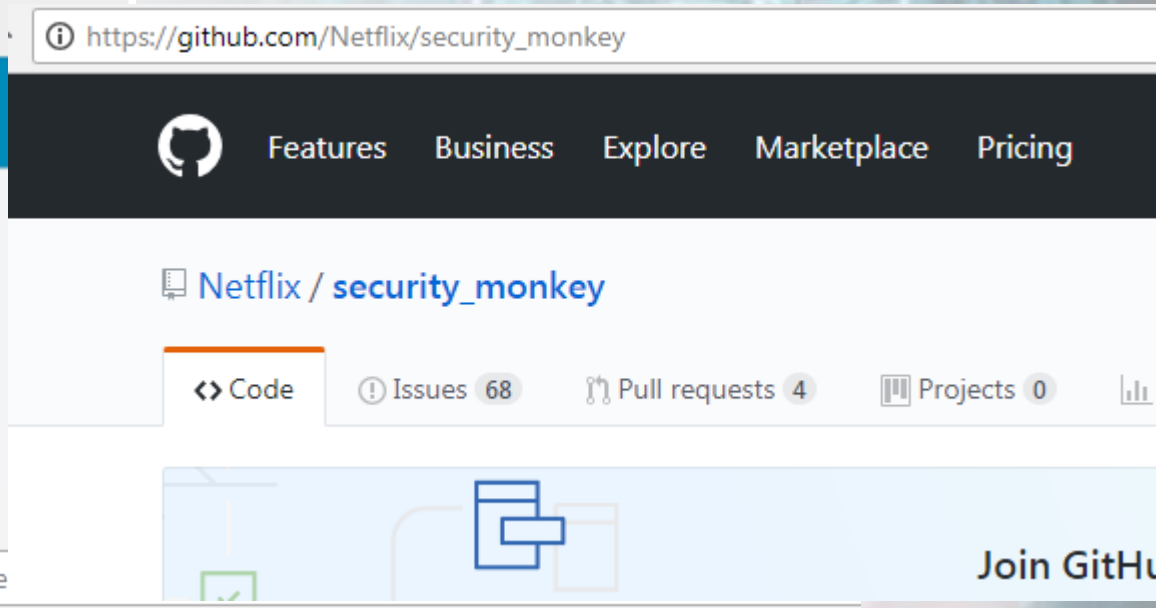
Security Monkey

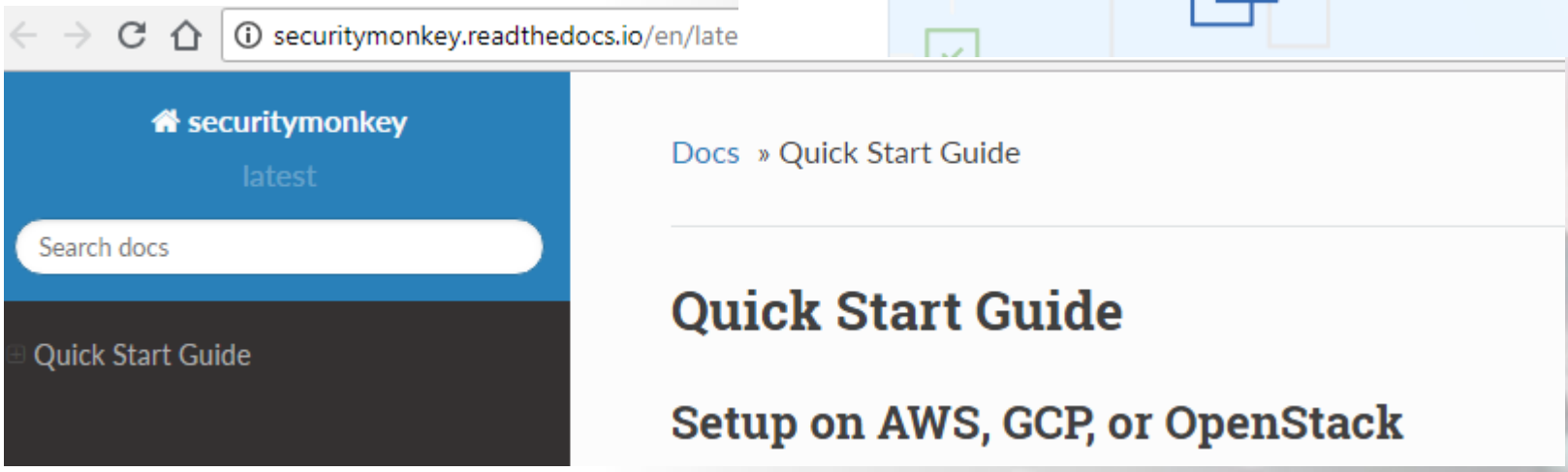
open source cloud security tracking system

Watcher, es el encargado de observar nuestra cuenta para detectar cambios. Cuando eso ocurre, se almacena esa información en la base de datos interna.
Notifier, es el encargado de avisarnos cuando se produce un evento que podemos personalizar.
Auditor, es el encargado de realizar pruebas y revisiones sobre los elementos, reglas y políticas. Podemos definir aquello que no queremos que ocurra para que salte una alarma si se encuentra (como grupos de seguridad con puertos abiertos al mundo).

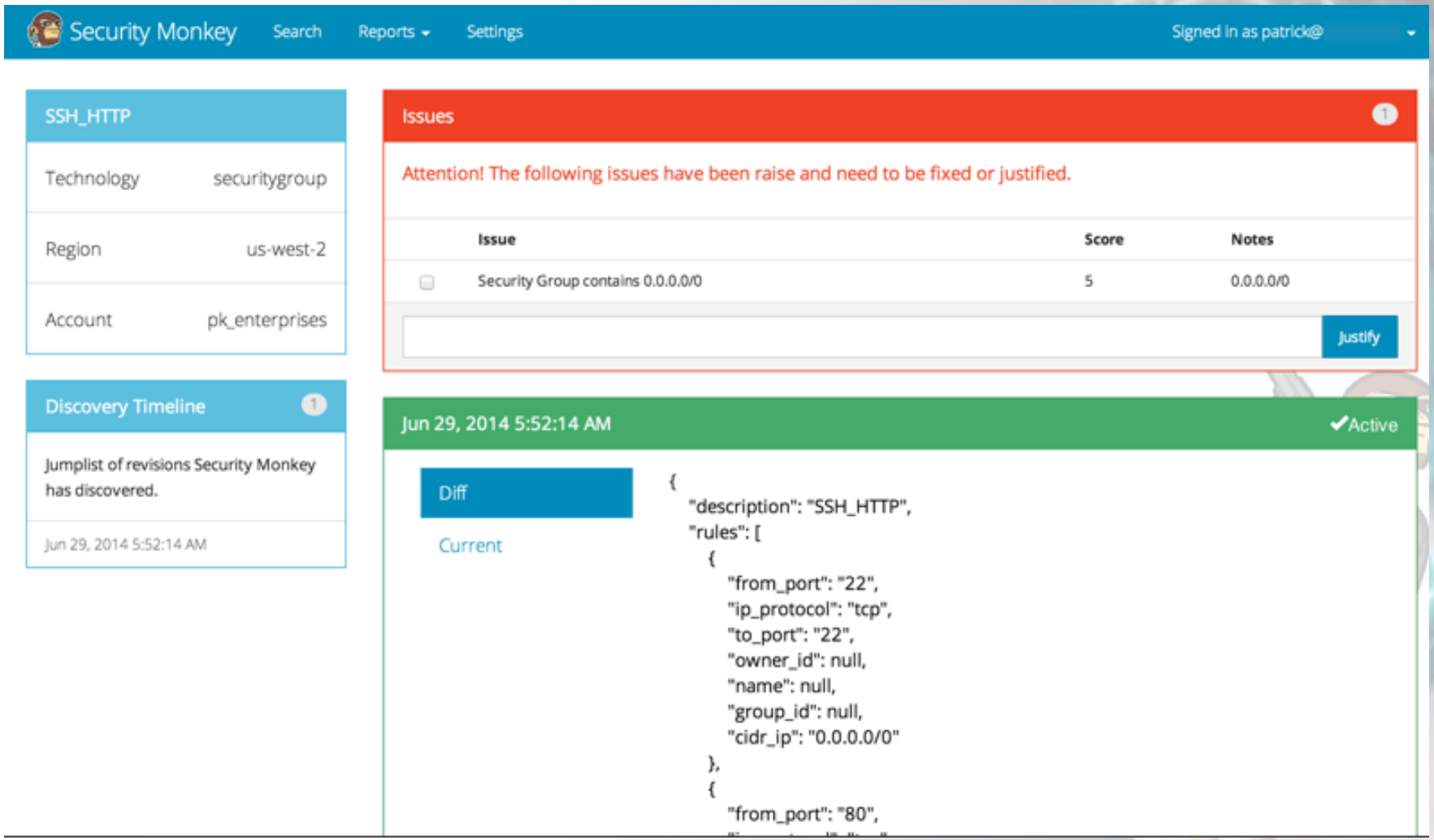
MSc. Ing. Guido Rosales



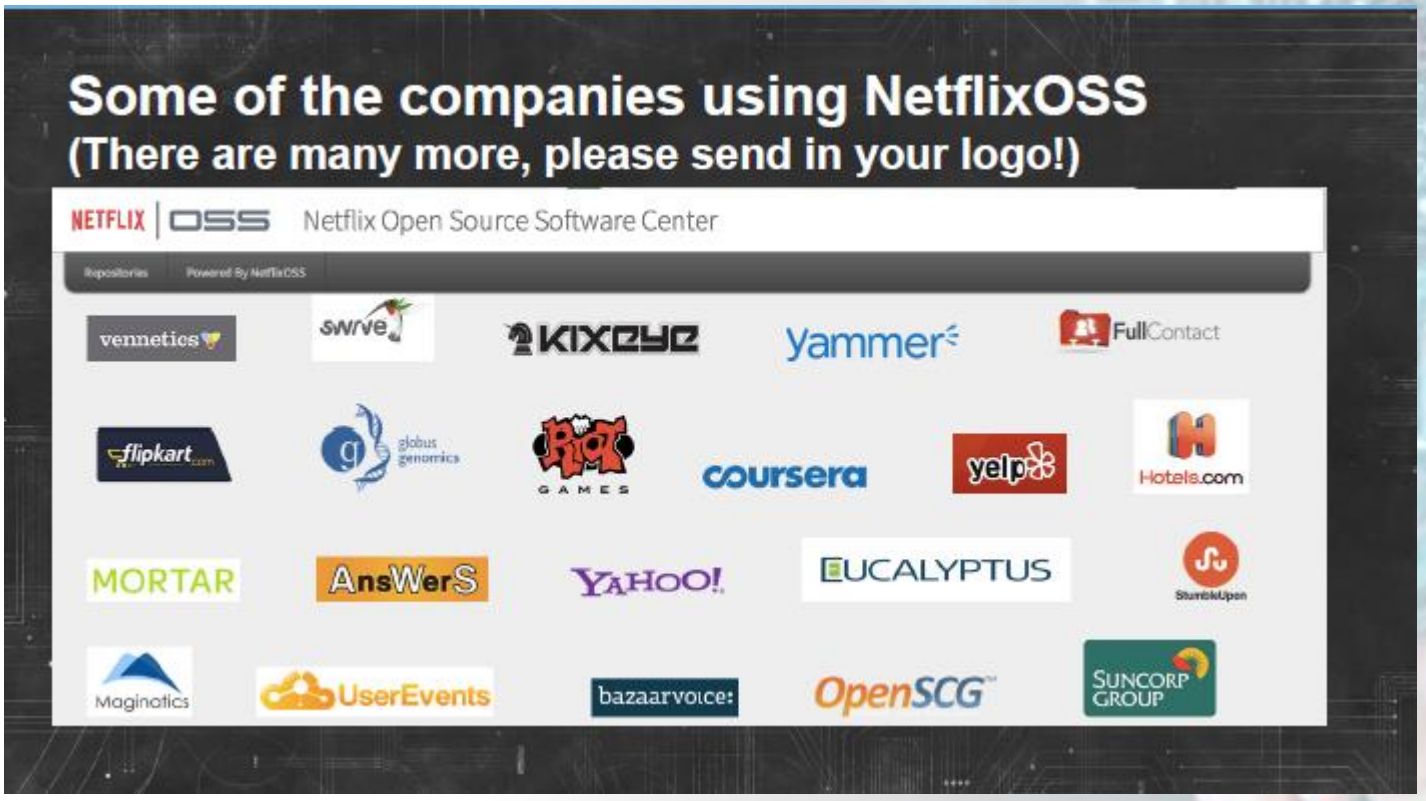




MSc. Ing. Guido Rosales

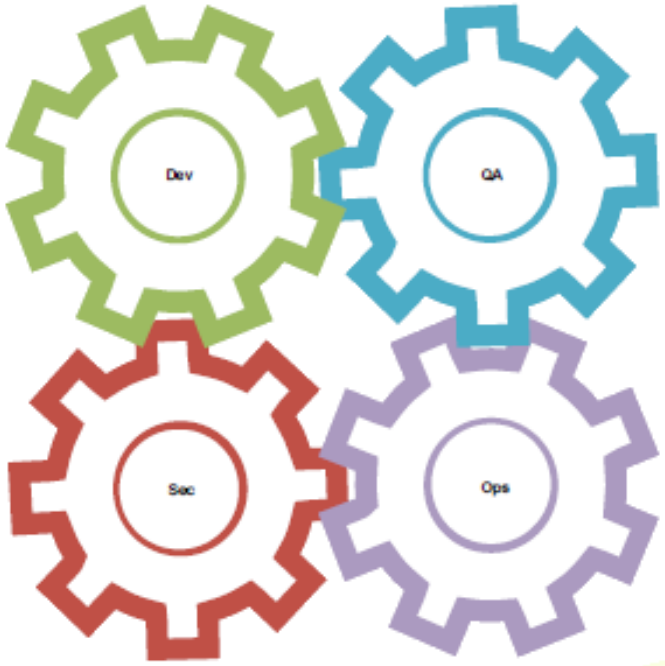


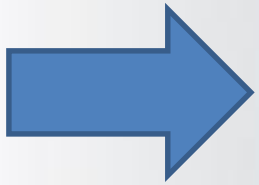
MSc. Ing. Guido Rosales


Some of the companies using NetflixOSS
(There are many more, please send in your logo!)
NETFLIX | OSS Netflix Open Source Software Center
Repositories
Powered By NetflixOSS
vennetics
swrve
KIXEYE
yammer
FullContact
flipkart.com
globus genomics
Riot GAMES
coursera
yelp
Hotels.com
MORTAR
AnswerS
YAHOO!
EUCALYPTUS
StumbleUpon
Maginatics
UserEvents
bazaarvoice
OpenSCG
SUNCORP GROUP

CONCLUSIONES

MSc. Ing. Guido Rosales





MSc. Ing. Guido Rosales

CONCLUSIONES

- La nube es un concepto. No es AWS o AZURE
- Las plataformas abiertas permiten aprender
- No todos deben implementar devsecops
  - Depende del tipo de negocio
- Pero todos deben comprender la **RESPONSABILIDAD TRANSVERSAL** sobre la seguridad
  - Clientes internos, desarrolladores, Operaciones

Desde el año 1999

Yanapti

CYBERSECURITY

MSc. Ing. Guido Rosales

TECNOLÓGICO SUPERIOR CORDILLERA

25 AÑOS

CIDE
Centro de Investigación y Desarrollo Ecuador

SEMINARIO INTERNACIONAL DE SEGURIDAD EN EL DESARROLLO DE SOFTWARE

WWW.CIDECUADOR.COM

Una vez finalizado el evento esta presentación sera publicada en su respectiva página web