



# DATOS 360°

Una visión integral para la gestión  
de los datos en el Estado




## Jornadas Tecnológicas

# La Importancia de los Datos en Ciberseguridad

Juan Pablo García

# La Importancia de los Datos en Ciberseguridad



Contar con datos de calidad en el momento y formato correcto en todas las disciplinas es un factor diferenciador para tomar decisiones, diseñar estrategias e innovar en servicios y productos.

En Ciberseguridad, además, son fundamentales para detectar ataques o eventos que puedan comprometer la seguridad de la información en todo el ecosistema.

Existen numerosas técnicas y tecnologías involucradas en la recolección y análisis de información, pero lo más importante es disponer de datos de calidad.

# Fuentes de Datos

## Colectores

### Sensores



## Ponderadores

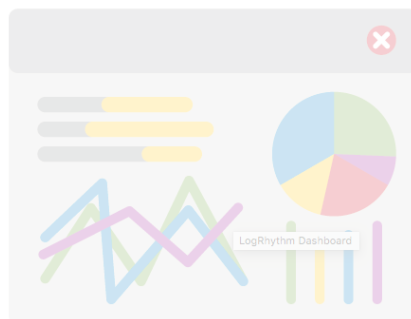


Fuentes de Inteligencia



Servicios Proactivos

Análisis de Datos  
en Tiempo Real  
24x7



SOC

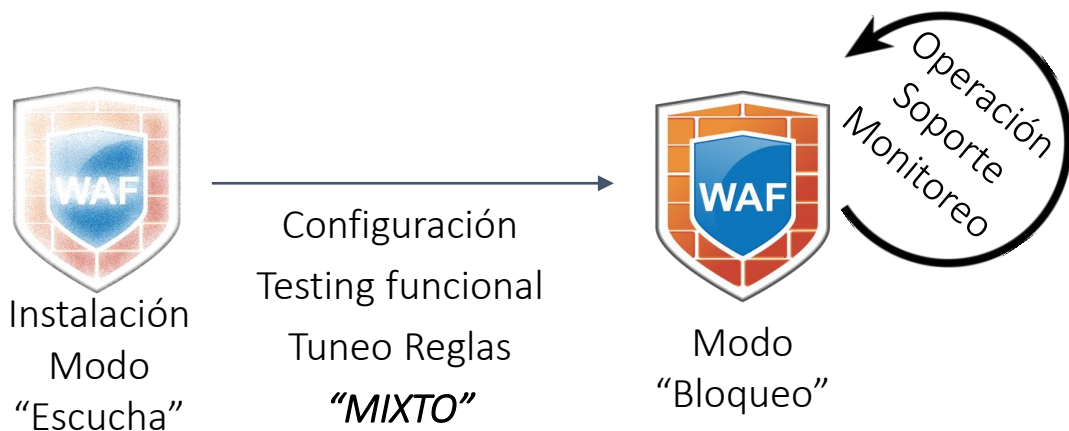
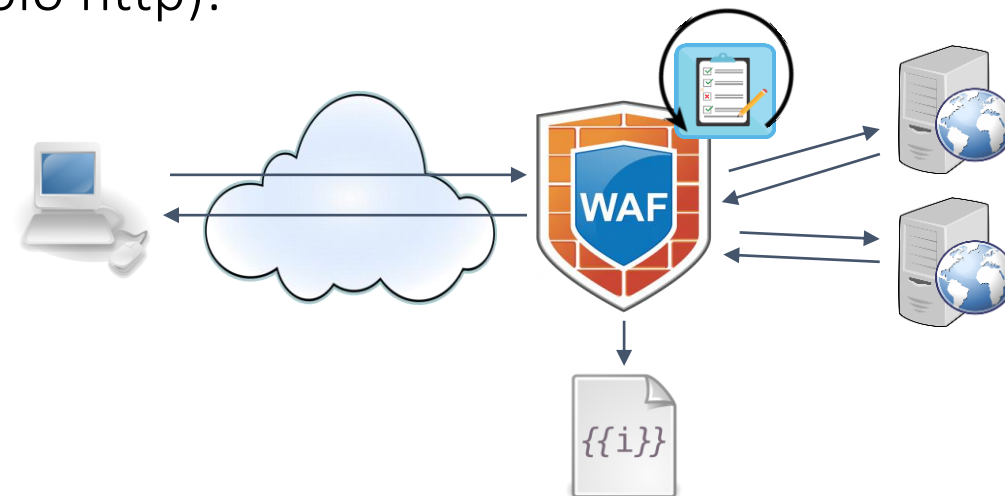


CERT

# Sensores / WAF (Web Application Firewall)

Firewall a nivel de aplicaciones / portales web (protocolo http):

- Bloquea en base a reglas;
- Informa mediante logs extendidos;
- Análisis continuo en modo pasivo;
- 4 modos: Escucha, Bloquea, Mixto, Puntaje;
- Reglas genéricas y específicas con alto grado de “tuneo”.



60 WAF funcionando en toda la  
Administración Central y otras organizaciones

# Sensores



Logs servidores



Firewalls (Reduy, RedSalud, LAN internas de Organismos)



N-IDS: detectores de intrusos a nivel de red



H-IDS: detectores de intrusos a nivel de servidor



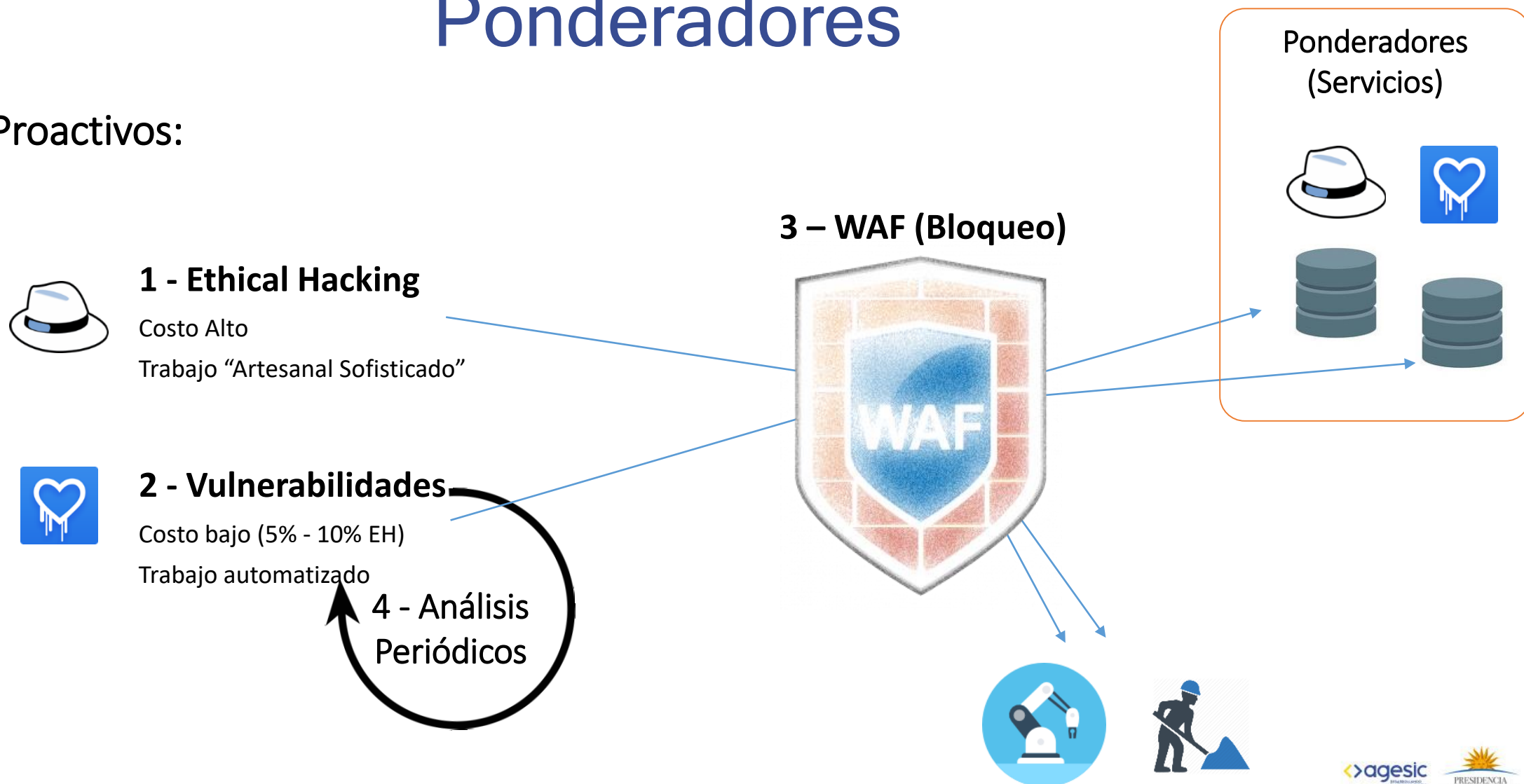
Nagios: detecta estados de webs, certificados, etc



Detección de defacement, open resolver, open relay, modificación de páginas web, palabras ofensivas.

# Ponderadores

## Servicios Proactivos:



# Ponderadores

## Servicios Proactivos:



### Ethical Hacking

+3.800 hs en 3 años

+11 vulnerabilidades críticas

+170 vulnerabilidades altas

## Fuentes de Inteligencia Internacionales:



Indicadores de Compromiso: listas de datos que permiten inferir (IPs, URLs, casillas de correo, etc)

*OTX (Alien Vault) - IBM Exchange – CERTs extranjeros – Twitter, hailataxii.com, virustotal.com, etc*

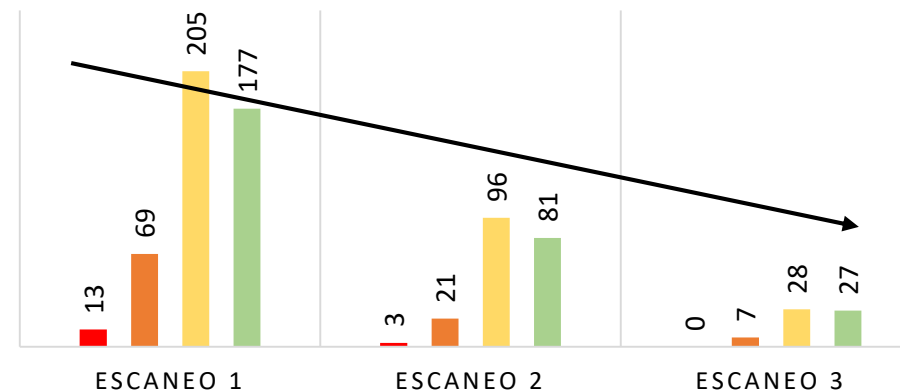


Threat Intelligence: inteligencia de amenazas (técnicas y herramientas de ataques que están ocurriendo)



### ANÁLISIS DE VULNERABILIDADES

■ Crítica ■ Alta ■ Media ■ Baja





# Situación Actual

## Colectores

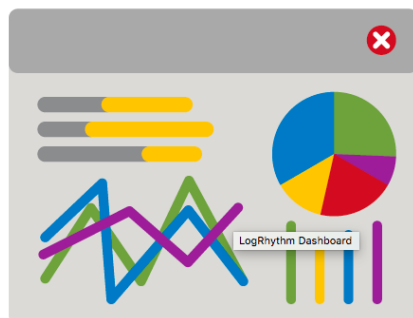
### Sensores



## Ponderadores



Análisis de Datos  
en Tiempo Real  
24x7 (SIEM)





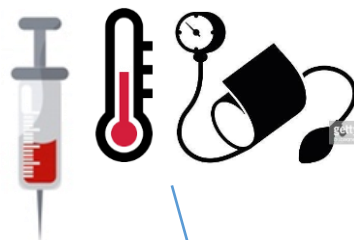
## En medicina...



- ✓ Prevenir mejor que curar
- ✓ Análisis periódicos (asintomáticos)
- ✓ Tecnología aplicada a los sensores (IoT)
- ✓ Análisis en tiempo real, automatización
- ✓ Ponderadores: HCE, IA para patrones y modelos de predicción, Big Data
- ✓ Ecosistema / Comunidad

### Colectores (Sensores):

- Temperatura
- Presión
- Imágenes
- Pulso
- Sangre
- Orina
- ...



### Ponderadores:

- Antecedentes (Historia Clínica)?
- Fuma?
- Hace deporte?
- Viajó? Comidas?
- Época del año?
- Epidemias?
- Estadística
- Experiencia



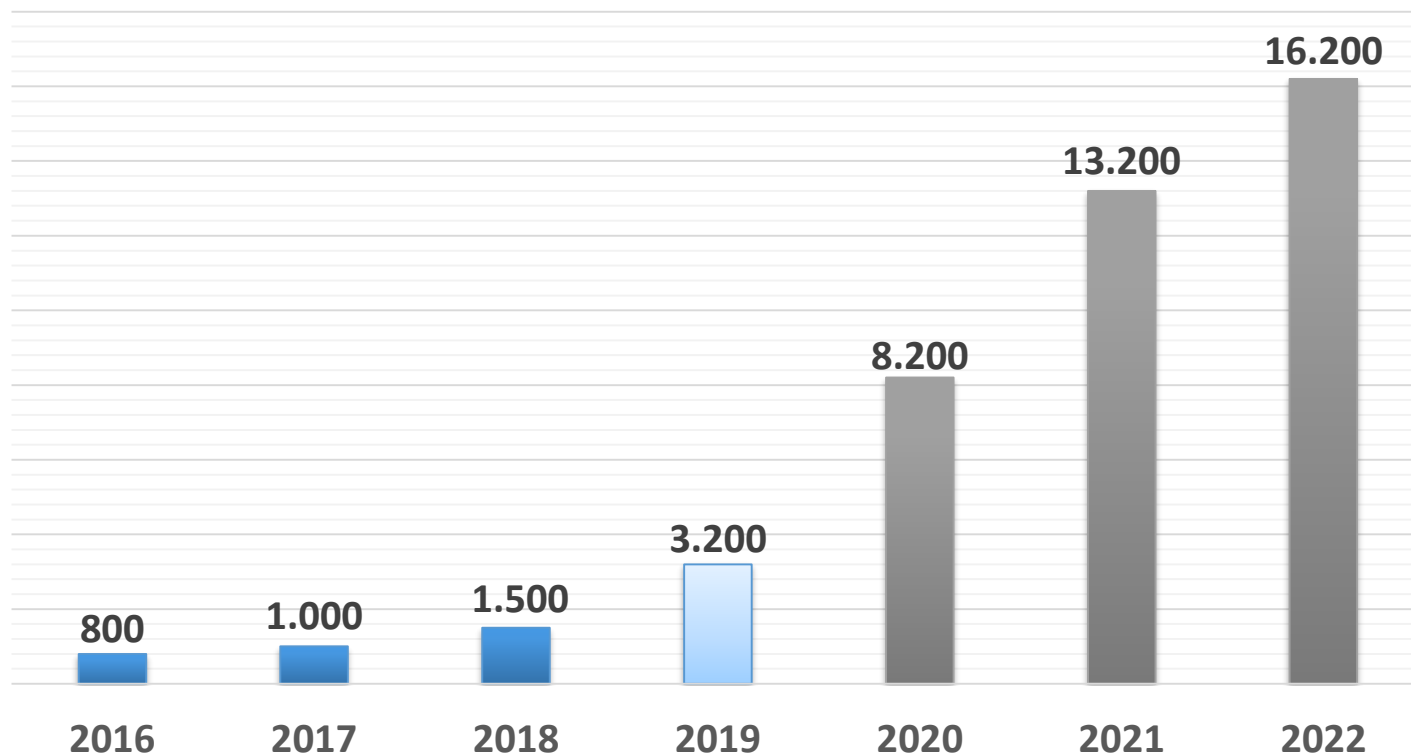
# Situación Actual

Algunos desafíos inmediatos:

- ✓ Gran cantidad de sensores, gestión compleja => **Automatización**
- ✓ Muchos datos, alta cantidad de falsos positivos => **Automatización y “tuneo” de sensores y análisis**
- ✓ Falta de profesionales especializados => **Aumentar la oferta académica, incentivar estudiantes**
- ✓ Poca **visibilidad / penetración**, demoras en las **respuestas**
- ✓ Más y mejor **Ecosistema**, nacional, regional, global
- ✓ Mayor capacidad de **análisis histórico** y uso de técnicas y tecnologías para **análisis predictivo**
- ✓ Baja percepción del **riesgo**

# Hacia el Big Data...

Registros Recolectados por Segundo



## Características del Big Data:

- ✓ Volumen
- ✓ Velocidad (cercano a tiempo real)
- ✓ Variedad de datos
- ✓ Veracidad de los datos (confianza)
- ✓ Viabilidad (explotación real)
- ✓ Visualización de los datos (efectiva)
- ✓ Valor de los datos (casos de negocio)

# Próximos Pasos

## Automatización:

- Gestión de Colectores
- Análisis de datos en tiempo real
- Respuestas

## Prevención:

- Más detecciones en forma temprana
- Gestión de Riesgos
- Marco de Ciberseguridad

## Ajustes:

- Menos falsos positivos
- Respuestas más rápidas

### Colectores

Desarrollo de Nuevos y Evolución  
Ampliar y profundizar detección

### Ponderadores

Nuevos IoC y Servicios



Ponderador

Análisis de Datos  
en Tiempo Real



### Análisis / Big Data / IA

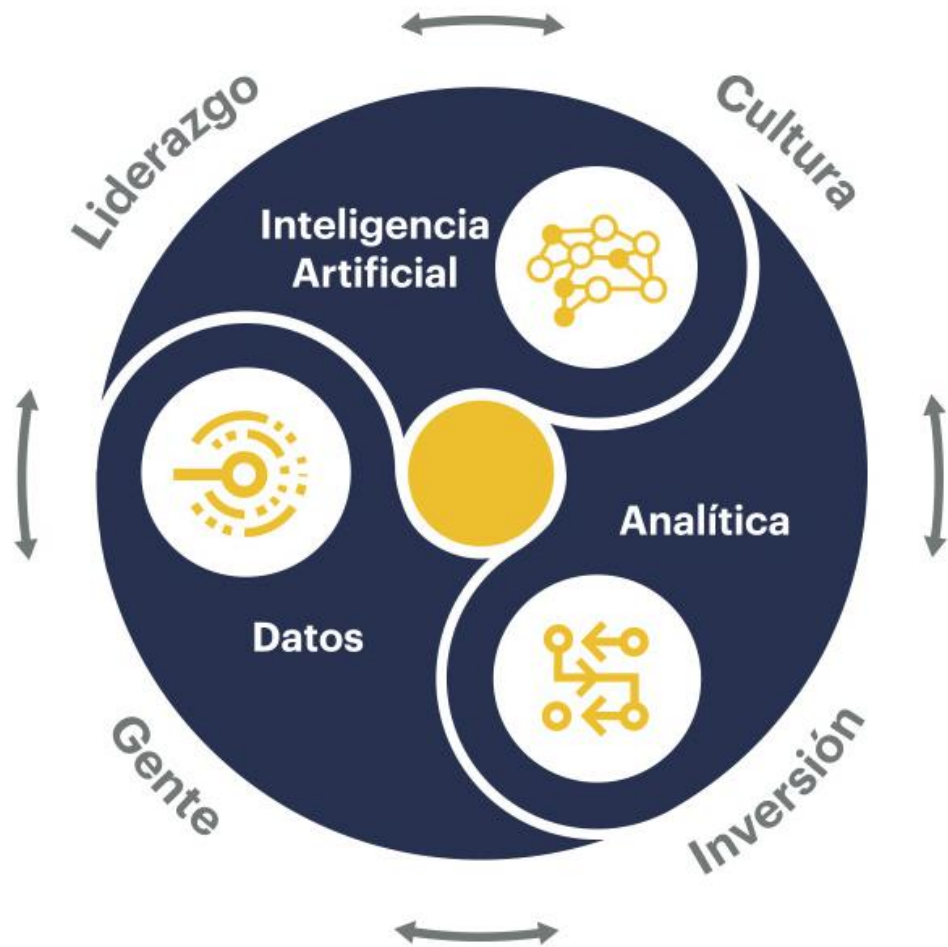
- ✓ Explotar más los **datos históricos**;
- ✓ **Inteligencia Artificial** para detectar patrones y modelos de predicción, etc.
- ✓ **Datos de valor anonimizados** para la industria, academia y otros CERT;
- ✓ **Datos para mejorar** gestión y servicios.

### Ponderador

Datos Ecosistema  
Comunidad Inter.



## Visión a Futuro



- ✓ Datos y Analítica (D&A) en el ADN de la organización;
- ✓ Calidad, Seguridad, Privacidad, Gobernanza;
- ✓ Fortalecer Ecosistema y Roles (“Chief Data Officer”, “Chief Analytics Officers” y CISO en Ciberseguridad);
- ✓ Explotación de datos al servicio de la innovación;
- ✓ Tecnologías emergentes: IA, Blockchain, IoT, Gemelos Digitales (Digital Twins), Analítica Aumentada, Reconocimiento Facial.
- ✓ Automatización;
- ✓ Lab -> PoC -> MVP. Desarrollo ágil e incremental de soluciones.

# ¡Gracias!

Juan Pablo García

[juanpablo.garcia@agesic.gub.uy](mailto:juanpablo.garcia@agesic.gub.uy)