



INCIDENTES EN LA NUBE... ¿Y AHORA QUÉ?, PUES FAAS

Lórien Doménech Ruiz

#CyberCamp17



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ENERGÍA, TURISMO
Y AGENDA DIGITAL

¿QUIÉN SOY?



- **Trabajo: Responsable Global del Servicio Digital Forense en Prosegur Ciberseguridad.**
- **Formación: Ingeniero Informático en Sistemas de la Información, y posteriormente, Máster en Informática Forense y Delitos Informáticos.**
- **Certificaciones que aplican: Microsoft MCP, Implementing Microsoft Azure Infrastructure Solutions, Certified Solutions Associate in Office 365 (MCSA), Microsoft Dynamics, CEH v9 EC-Council.**
- **Director del área Forense y Delegado de Madrid por la asociación @StopVGDigital**
- **Profesor invitado de Ciberseguridad en la Escuela Técnica EADIC (@eadic).**
- **Grupos y actividades: #Cibercooperantes, @Cibervoluntario, y @Hack4ensicTeam_**

ÍNDICE



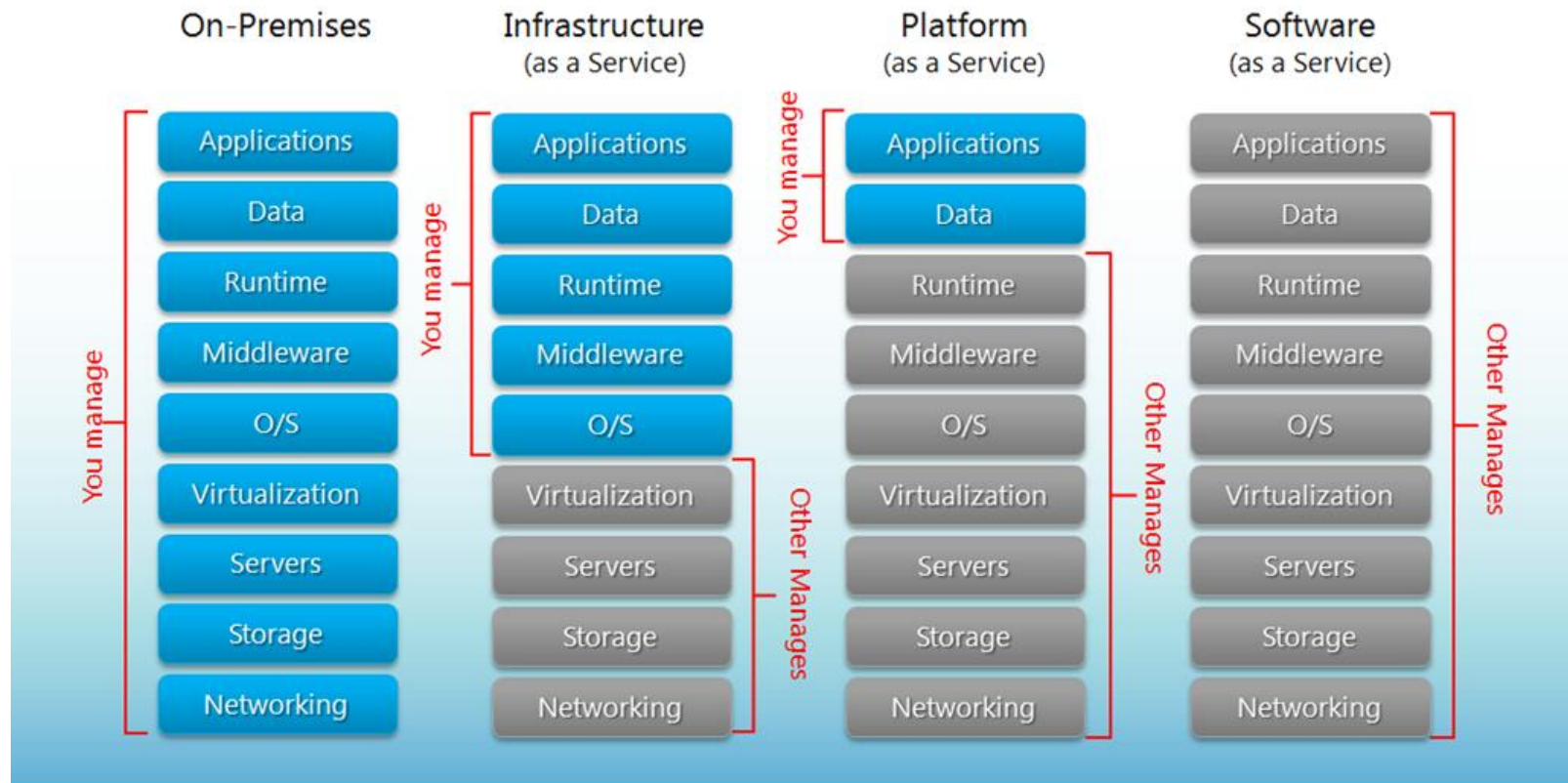
- 1. Conceptos generales de FAAS.**
- 2. Captación de evidencias dependiendo de la arquitectura.**
- 3. Resolución de incidencias.**
- 4. Crear un entorno de análisis forense en la nube.**
- 5. Análisis de las evidencias en el laboratorio en la nube.**
- 6. Conclusiones.**



CONCEPTOS GENERALES DE FAAS

Modelo de Servicio (SaaS, PaaS, IaaS) y el FaaS

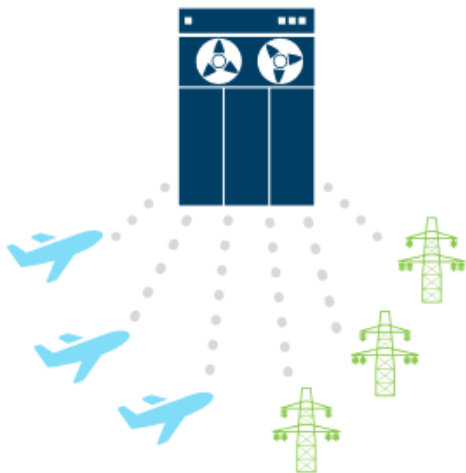
Separation of Responsibilities



Fuente: apprenda.com

CONCEPTOS GENERALES DE FAAS

Before 2005



Closed and centralized
IoT networks

Today



Open access IoT networks,
centralized cloud

2025 and beyond



Open access IoT networks,
distributed cloud

Fuente: nycla.org



CAPTACIÓN DE EVIDENCIAS DEPENDIENDO DE LA ARQUITECTURA

Algunos proveedores nos dicen que la nube es 100% segura. ¿Es verdad?

Incidentes que pueden arruinar a una empresa:

- Instancias comprometidas
- Mal desarrollo e implantación
- Mala praxis de usuarios
- Exposición de claves
- Ataques combinados

Los retos para ofrecer el servicio:

Relación con el Proveedor, Permisos, Características, Jurisdicción, Integridad, Preservación – CDC.

Preparación del FaaS:

Estudio de la Arquitectura implementada, Estudio legal, Discos virtuales implicados, BBDD y localización, otros EndPoints, perfil de auditor, SLAs, recursos forenses y costes, cierre del contrato.



CAPTACIÓN DE EVIDENCIAS DEPENDIENDO DE LA ARQUITECTURA



CREAR METODOLOGÍA Y ENTORNO DE ANÁLISIS FORENSE EN LA NUBE.



Toma de decisión sobre el método de actuación sobre la infraestructura del cliente/proveedor, con sus pros y contras:

➤ **Forense en la nube con una instancia específica**

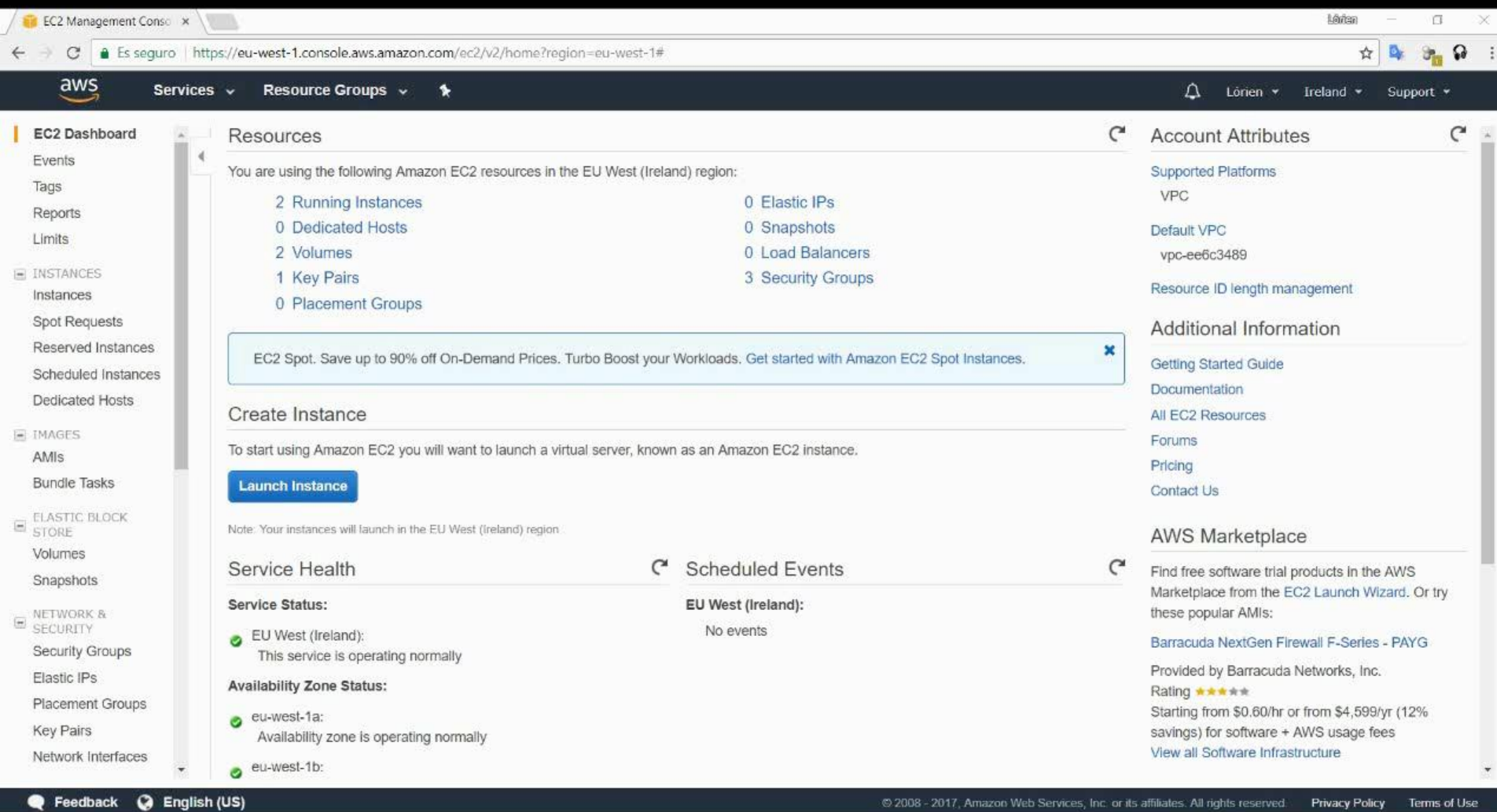
- Demo – creación de un entorno forense: Sift (Sans) en AWS y posterior enlace de evidencias para su procesamiento.

➤ **Traslado de las evidencias a un entorno de Forense tradicional**

- Demo – extracción de memoria RAM y artefactos de una máquina Windows en Azure, con un posterior análisis forense.
- Demo – extracción de evidencias de una máquina Red Hat 7 en GCP para su análisis forense.



Demo-creación de un entorno forense Sift en AWS



The screenshot displays the AWS Management Console for the EU West (Ireland) region. The left sidebar shows navigation options like EC2 Dashboard, INSTANCES, IMAGES, ELASTIC BLOCK STORE, and NETWORK & SECURITY. The main content area is divided into several sections:

- Resources:** Lists EC2 resources in the EU West (Ireland) region: 2 Running Instances, 0 Elastic IPs, 0 Dedicated Hosts, 0 Snapshots, 2 Volumes, 0 Load Balancers, 1 Key Pairs, 3 Security Groups, and 0 Placement Groups.
- Create Instance:** A section with a "Launch Instance" button and a note that instances will launch in the EU West (Ireland) region.
- Service Health:** Shows the status of the EU West (Ireland) service as "operating normally" and the availability zones (eu-west-1a and eu-west-1b) as "operating normally".
- Scheduled Events:** Indicates "No events" for the EU West (Ireland) region.
- Account Attributes:** Displays supported platforms (VPC), default VPC (vpc-ee6c3489), and resource ID length management.
- Additional Information:** Links to Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing, and Contact Us.
- AWS Marketplace:** Promotes free software trial products from the EC2 Launch Wizard, specifically mentioning Barracuda NextGen Firewall F-Series - PAYG.

The bottom of the console features a footer with "Feedback", "English (US)", and copyright information for Amazon Web Services, Inc. (© 2008 - 2017).

Demo – extracción de memoria RAM y artefactos en Azure



Microsoft Azure nav2015

Search resources, services and docs

nav2015 Virtual machine

Connect Start Restart Stop Move Delete Refresh

Failed

Resource group (change) [nav](#)

Status Failed

Location North Europe

Subscription (change) [BizSpark](#)

Subscription ID XXXXXXXXXX

Computer name nav2015

Operating system Windows

Size Standard D1 (1 vcpu, 3.5 GB memory)

Public IP address 40.69.87.138

Virtual network/subnet [nav-vnet/default](#)

DNS name [hhdemo.northeurope.cloudapp.azure.com](#)

Show data for last: 1 hour 6 hours 12 hours 1 day 7 days 30 days

CPU (average)

100% 80% 60% 40% 20% 0%

11:30 AM 11:45 AM 12 PM 12:15 PM

PERCENTAGE CPU 1.19 %

Network (total)

1,000kB 800kB 600kB 400kB 200kB 0kB

11:30 AM 11:45 AM 12 PM 12:15 PM

NETWORK IN 20.99 MB NETWORK OUT 38.55 MB

Demo – extracción de un disco duro en GCP



Soluciones de Cloud Lau x 4ensic Segmento - My f x

Es seguro | <https://console.cloud.google.com/launcher?project=optimum-airfoil-187216&hl=es>

Tu crédito actual es de 251,40 € y quedan 361 días para que finalice el periodo de prueba gratuita.

IGNORAR ACTUALIZAR

Google Cloud Platform My First Project

Explora, activa y administra soluciones con tan solo unos clics
Con Cloud Launcher puedes desplegar software rápidamente en Google Cloud Platform

Buscar soluciones

Ver todas las soluciones Recomendadas

Tus soluciones

Filtrar por

- Máquinas virtuales (307)
- Google Cloud Platform (38)
- APIs y servicios (248)
- Contenedores (25)
- Conjuntos de datos (79)
- Sistemas operativos (30)
- Pilas desarrolladores (82)
- Redes (58)
- Bases de datos (59)

Destacadas

| WordPress | App Engine | Compute Engine | Windows Server 2016 | LAMP |
|---|---|---|--|--|
| Google Click to Deploy | Google | Google | Microsoft | Bitnami |
| Web publishing platform for building blogs and websites | Una plataforma para crear aplicaciones web y móviles que se | Máquinas virtuales escalables de alto rendimiento | Windows Server 2016 Datacenter Edition | Infrastructure software from the leading publisher |
| Tipo Máquinas virtuales | Tipo Google Cloud Platform | Tipo Google Cloud Platform | Tipo Máquinas virtuales | Tipo Máquinas virtuales |

RESOLUCIÓN DE INCIDENCIAS



Tareas a realizar según el caso,
Objetivo: automatizar



Fuente: @ToniBlyx – RootedCon2017

CONCLUSIONES



■ Desde el punto de vista del cliente:

- El planteamiento inicial de los entornos en la nube desde el punto de vista de la seguridad de la información.
- Tener un sistema de alteras sobre sus sistemas muy afinado y según el proveedor.
- Tener un sistema de gestión de claves eficaz y controlar el desempeño de los desarrolladores.

■ Desde el punto de vista del servicio FaaS:

- Visión total y permisos pertinentes sobre las instancias del cliente.
- Tener un pool de recursos con capacidad de adaptación al contexto del incidente.
- Conocimiento de herramientas propietarios vs software libre.
- Formación continua y siempre que se pueda certificada.
- Suscripción a los boletines de seguridad y nuevos evolutivos.



Gracias por su atención

Lórien Doménech Ruiz

Responsable Global del Servicio Digital Forense de
Prosegur Ciberseguridad

- ✓ lorien.domenech@prosegur.com
- ✓ <https://es.linkedin.com/in/loriendr>
- ✓ <https://github.com/loriendr>
- ✓ @loriendr



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ENERGÍA, TURISMO
Y AGENDA DIGITAL

 **incibe**
INSTITUTO NACIONAL DE
CIBERSEGURIDAD