

Grado en Ingeniería Informática

Sistemas distribuidos

# Seguridad en sistemas distribuidos

Víctor Vives

[vvives@dtic.ua.es](mailto:vvives@dtic.ua.es)

Departamento de Tecnología Informática y Computación

2021 - 2022

# 1. Introducción

---

## 1. Introducción

## 2. Requerimientos

## 3. Vulnerabilidades

## 4. Ataques

## 5. PaaS

### Seguridad en sistemas distribuidos

El objetivo principal de seguridad es **restringir el acceso a la información** y los recursos de modo que solo tengan **acceso** aquellos que estén **autorizados**

### Niveles de atención

Hay que diferenciar entre **seguridad de la información** y la **seguridad del sistema en general**

Definición de **políticas de seguridad** y construcción de **mecanismos de seguridad**

# 1. Introducción

---

1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS



<https://cve.mitre.org/>

## 2. Requerimientos

---

1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS

### Requerimientos del atacante

#### Servicio orientado a Internet

Muchas de las vulnerabilidades registradas en el CVE pueden ser potencialmente explotables por un atacante remoto si se está conectado a Internet. El atacante no necesariamente debe disponer de privilegios de acceso, el único requerimiento es que el atacante pueda descubrir el servicio y enviar mensajes por red.

#### Acceso local o remoto al servicio

Esta condición requiere que el atacante tenga ciertos privilegios que le permitan un acceso lógico a servicios o funciones de un dispositivo o máquina. El acceso lógico puede estar restringido a acceso local o puede ser de forma remota (p.ej. vía Internet). A menudo estos privilegios requeridos son privilegios de usuarios normales y no de administrador.

## 2. Requerimientos

---

1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS

### Requerimientos del atacante

#### Acceso físico directo al dispositivo

El atacante requiere acceso físico directo al dispositivo o máquina. Sin embargo, no necesariamente requiere de privilegios o acceso a los servicios.

#### Proximidad física del atacante

En algunos casos el atacante no necesita acceso físico a un dispositivo o máquina, es suficiente con estar próximo físicamente a cualquiera. En muchos casos esta proximidad la marca el rango de radio del dispositivo o máquina.

#### Miscelánea

Condiciones que aparecen una o dos veces en los registros de CVE.

Un ejemplo de condición miscelánea es que el servicio o librería esté en una determinada versión o configurado de cierta manera para que la vulnerabilidad sea explotable.

## 2. Requerimientos

---

1. Introducción

2. Requerimientos

3. Vulnerabilidades

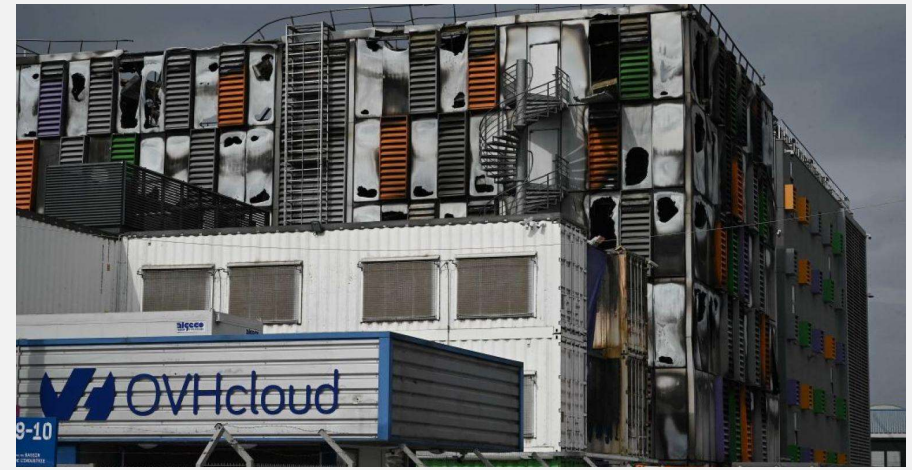
4. Ataques

5. PaaS

### Incendio del principal *datacenter* en OVHcloud (marzo 2021)

[Enlace a la noticia: no revelarán el motivo del incendio hasta 2022](#)

[Enlace a la noticia: El pasado mes \(13 de octubre\) recibieron un ataque DDoS](#)



## 3. Vulnerabilidades

---

1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS

### Vulnerabilidades más comunes

#### Errores de programación

Muchas vulnerabilidades en los registros del VCE hacen referencia a errores de programación que permiten ataques de control de flujo, como por ejemplo vulnerabilidades en el análisis y validación de los datos de entrada o mala gestión de memoria al liberar punteros.

#### Vulnerabilidad basada en web

Muchos dispositivos o máquinas tienen interfaces de gestión desde las que se permiten accesos para poder configurar o actualizar un dispositivo, máquina o determinados servicios o funciones.

#### Autenticación o controles de acceso débiles

Contraseñas por defecto o débiles. Algunos dispositivos o servicios tienen contraseñas “hardcoded” o “a fuego” que proporcionan accesos por puertas traseras. Este tipo de vulnerabilidades permiten al atacante hacer un bypass de los mecanismos de control de acceso de forma muy sencilla y con mínimo esfuerzo.

## 3. Vulnerabilidades

1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS

### Errores de programación



### Un murciano recibe una factura telefónica de 19.500 euros tras enviar 100.000 SMS por un error de su compañía

EFE NOTICIA 30.10.2021 - 17:38H

La empresa llegó a cortar la línea móvil y a amenazarle con llevarlo al registro de morosos.



### You knitwits! Couple with KN19 TER number plate on their car get hit with £90 fine... thanks to woman in 'Knitter' shirt walking along bus lane

- David Knight, 54, from Dorking, Surrey, received a fine for driving down a bus lane in Bath - but the builder immediately knew there had been a mistake
- He and his wife, Paula, 54, looked at photographic evidence which showed a woman walking in the bus lane with the wrong registration plate
- The council computer mixed up the words 'knitter' and 'knitter' on Mr Knight's Volkswagen

By LIZ HULL FOR THE DAILY MAIL

PUBLISHED: 22:49 GMT, 17 October 2021 | UPDATED: 23:00 GMT, 17 October 2021





## 3. Vulnerabilidades

---

1. Introducción

2. Requerimientos

**3. Vulnerabilidades**

4. Ataques

5. PaaS

### Vulnerabilidades más comunes

#### Uso inapropiado de la criptografía

Algunos servicios utilizan mecanismos de criptografía con propósitos de autenticación de usuarios o para preservar la confidencialidad de determinada información sensible o confidencial. A menudo, estos mecanismos de criptografía no se utilizan de forma apropiada y terminan provocando fallos de seguridad fatales.

Un ejemplo es el uso de generadores de números aleatorios para generar claves criptográficas o varias vulnerabilidades en protocolos que utilizan primitivas criptográficas.

#### Miscelánea

Otras vulnerabilidades que describen un determinado objetivo y el efecto de ataques potenciales sobre diferentes vulnerabilidades de ese objetivo.

## 4. Ataques

---

1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS

### Tipos de ataque

#### Secuestro de sesión o *hijacking*

En este tipo de ataques se desvía el flujo de control normal de los programas que se ejecutan en un dispositivo o máquina, lo que suele resultar en la ejecución de código inyectado por el atacante.

#### Ingeniería inversa

Un atacante puede obtener información confidencial o vulnerabilidades a partir del código analizando el software (*firmware* o aplicación) de un dispositivo o servicio utilizando técnicas de ingeniería inversa.

#### Inyección de paquetes

Los ataques mediante inyección de paquetes aprovechan diferentes vulnerabilidades de análisis en implementaciones de protocolos u otros programas.

## 4. Ataques

---

1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS

### Tipos de ataque

#### *Eavesdropping* o escucha secreta

Mientras que la inyección de paquetes es un método de ataque activo, el *eavesdropping* junto con el *sniffing* son métodos de ataque pasivos que consisten en obtener los mensajes que se envían y se reciben en un dispositivo.

#### Ataque por fuerza bruta

Una criptografía o un método de autenticación débil puede romperse utilizando ataques por fuerza bruta. Este tipo de ataques consiste en una búsqueda exhaustiva de búsqueda de claves contra algoritmos de cifrado o funciones MAC. Requieren de un espacio de búsqueda de soluciones pequeño.

#### Uso normal

Este ataque hace referencia a un ataque que explota un servicio protegido haciendo un uso normal del mismo. Es decir, que no existe un mecanismo de control de acceso en el servicio.

## 4. Ataques

---

1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS

### Tipos de ataque

#### Denegación de servicio

La denegación de un servicio puede ser un mal funcionamiento del servicio o la detención completa del servicio.

#### Ejecución de código

El efecto de muchos ataques es la ejecución de código proporcionado por el atacante en el servicio. Esto incluye tanto scripts como inyecciones, no únicamente código nativo de la aplicación.

#### Violación de la integridad

Otro efecto muy común en los ataques es la violación de la integridad de los datos o del código en el servicio. Esto incluye la modificación de archivos y ajustes de configuración, así como la actualización ilegítima del firmware o algunas aplicaciones.

## 4. Ataques

---

1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS

### Tipos de ataque

#### Fuga de información

En algunos casos, el efecto del ataque es la filtración de cierta información que el atacante no debería obtener.

#### Acceso ilegítimo

Muchos ataques hacen que el atacante obtenga acceso ilegítimo al dispositivo. Esto no solo incluye los casos en los que un atacante, que de otro modo no tiene acceso al dispositivo, logra entrar lógicamente en él, sino también los casos en los que el atacante ya tiene algún acceso, pero obtiene más privilegios.

#### Pérdida financiera

Ciertos ataques permiten que el atacante cause pérdidas económicas a la víctima. La mayoría de los ataques pueden provocar pérdidas económicas en un sentido general, por lo que utilizamos este criterio para representar solo aquellos ataques cuyo objetivo principal es causar pérdidas financieras.

## 4. Ataques

---

1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS

### Tipos de ataque

#### Nivel de protección degradado

El ataque da como resultado un nivel de protección más bajo de lo esperado. Un ejemplo sería cuando se engaña a un dispositivo para que utilice algoritmos o políticas de seguridad más débiles que las que realmente admite.

#### Miscelánea

Algunos ataques hacen que los usuarios sean redirigidos a sitios web maliciosos o que se redirija el tráfico. En estos casos, no hay suficiente información sobre lo que sucede exactamente con el usuario o el tráfico redirigido.

## 4. Ataques

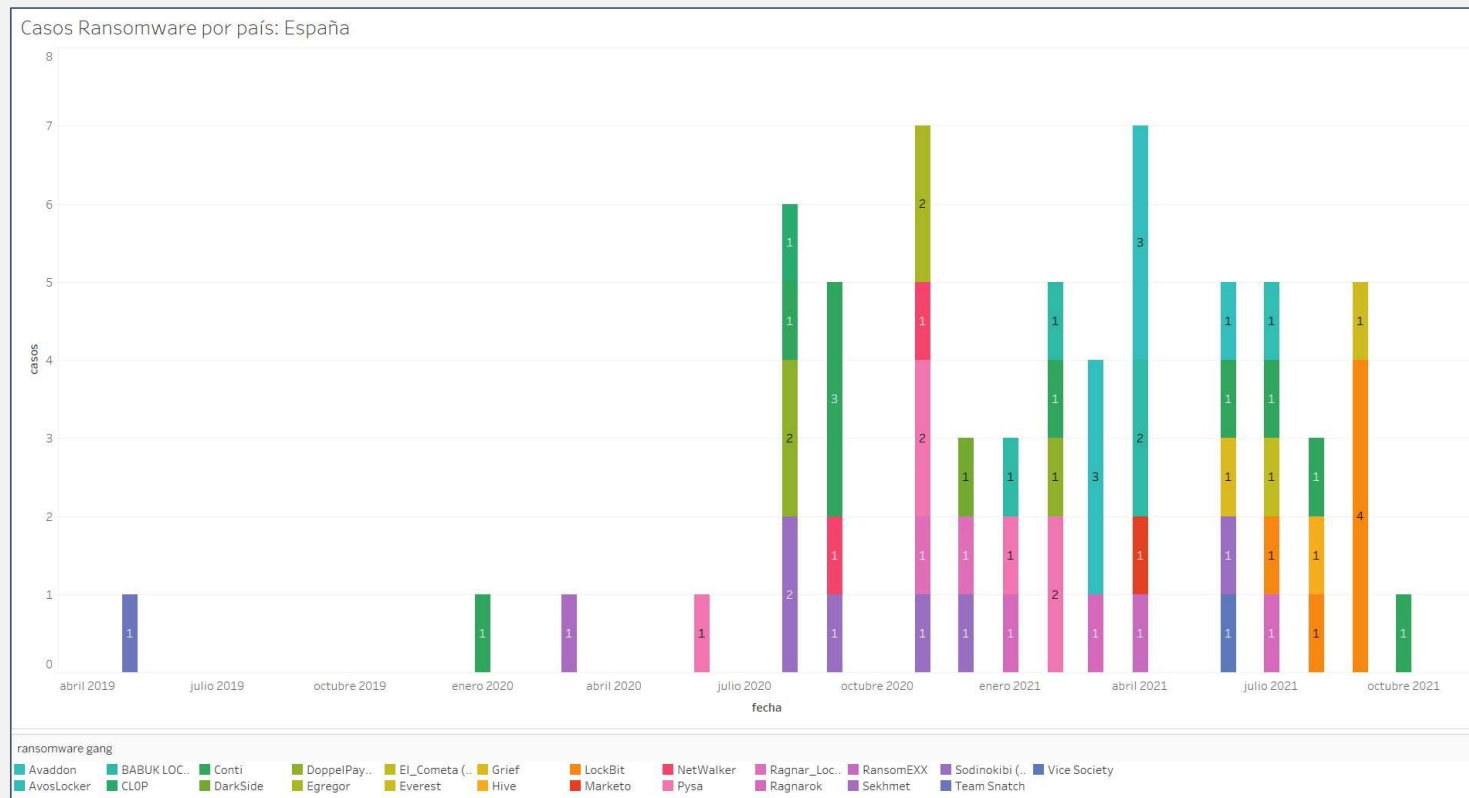
1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS



## 4. Ataques

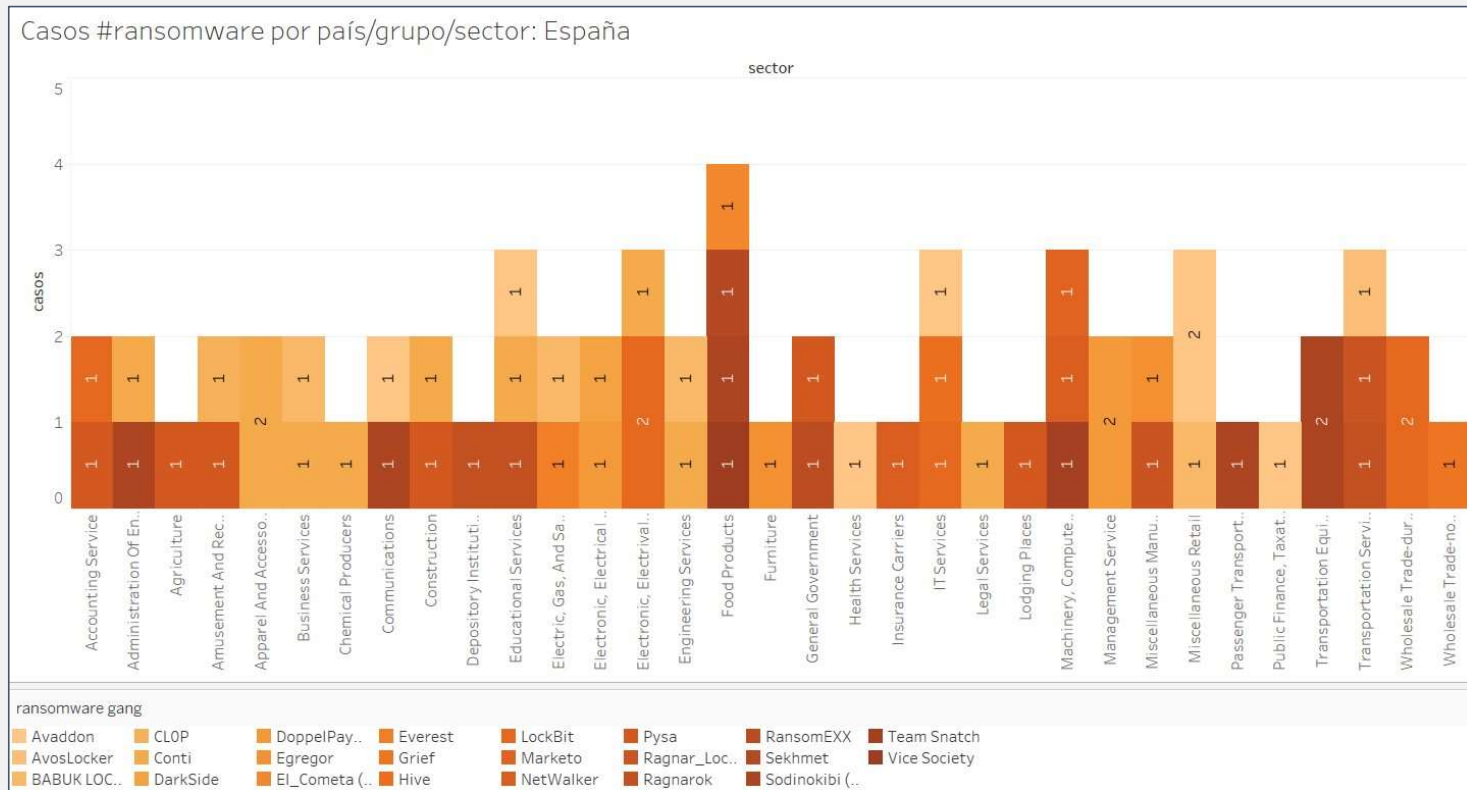
1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS





## 4. Plataforma como servicio

1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS

### Amazon Web Services

<b>Amazon Cloud Directory</b> Cree directorios flexibles nativos en la nube	<b>Amazon Cognito</b> Administración de identidades para las aplicaciones	<b>Amazon GuardDuty</b> Servicio administrado de detección de amenazas
<b>Amazon Inspector</b> Analice el nivel de seguridad de las aplicaciones	<b>Amazon Macie</b> Descubra, clasifique y proteja sus datos	<b>AWS Certificate Manager</b> Aprovisionamiento, administración e implementación de certificados SSL/TLS
<b>AWS CloudHSM</b> Almacenamiento de claves en hardware a efectos de conformidad normativa	<b>AWS Directory Service</b> Hospede y administre Active Directory	<b>AWS Firewall Manager</b> Administración centralizada de reglas de Firewall
<b>AWS Secrets Manager</b> Alterne, administre y recupere datos confidenciales	<b>AWS Security Hub</b> Centro unificado de seguridad y conformidad	<b>AWS Key Management Service</b> Creación y control administrados de claves de cifrado
<b>AWS Shield</b> Protección frente a ataques DDoS	<b>AWS WAF</b> Filtre el tráfico web malintencionado	

## 4. Plataforma como servicio

1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS

### Amazon Web Services

Precios	AWS Shield Standard	AWS Shield Advanced
Compromiso de suscripción	Ninguno	1 año*
Tarifa mensual (ver nota 1)	Sin costo adicional	3.000,00 USD
Tarifas de uso de la transferencia de datos de salida (ver nota 2)	Sin costo adicional	Las tarifas de uso de transferencia de datos de AWS Shield Advanced se aplican según la siguiente tabla.

#### Tarifas de uso de la transferencia de datos de salida de AWS Shield Advanced (por GB)

	Amazon CloudFront	Elastic Load Balancing (ELB)	IP elástica de AWS (EC2 y Balanceador de carga de red)	AWS Global Accelerator	Amazon Route 53
Primeros 100 TB	0,025 USD	0,05 USD	0,05 USD	0,05 USD	Sin costo adicional
Siguientes 400 TB	0,02 USD	0,04 USD	0,04 USD	0,04 USD	Sin costo adicional
Siguientes 500 TB	0,015 USD	0,03 USD	0,03 USD	0,03 USD	Sin costo adicional
Siguientes 4 PB	0,01 USD	<a href="#">Contacte con nosotros</a>	<a href="#">Contacte con nosotros</a>	<a href="#">Contacte con nosotros</a>	Sin costo adicional
Más de 5 PB	<a href="#">Contacte con nosotros</a>	<a href="#">Contacte con nosotros</a>	<a href="#">Contacte con nosotros</a>	<a href="#">Contacte con nosotros</a>	Sin costo adicional

## 4. Plataforma como servicio

1. Introducción

2. Requerimientos

3. Vulnerabilidades

4. Ataques

5. PaaS

### Microsoft Azure



#### Azure Sentinel

Utilice la funcionalidad SIEM nativa en la nube y análisis de seguridad inteligentes para mejorar la protección de su empresa.



#### Key Vault

Proteja y mantenga el control de las claves y otros secretos



#### Application Gateway

Cree front-ends web seguros, escalables y de alta disponibilidad en Azure



#### Azure Dedicated HSM

Administre los módulos de seguridad de hardware que utiliza en la nube



#### VPN Gateway

Establecer conectividad segura entre entornos locales



#### Azure Active Directory

Sincronice los directorios locales y habilite el inicio de sesión único



#### Azure DDoS Protection

Proteja sus aplicaciones frente a ataques por denegación de servicio distribuido (DDoS)



#### Azure Defender

Proteja las cargas de trabajo de nube híbrida

## 4. Plataforma como servicio

1. Introducción

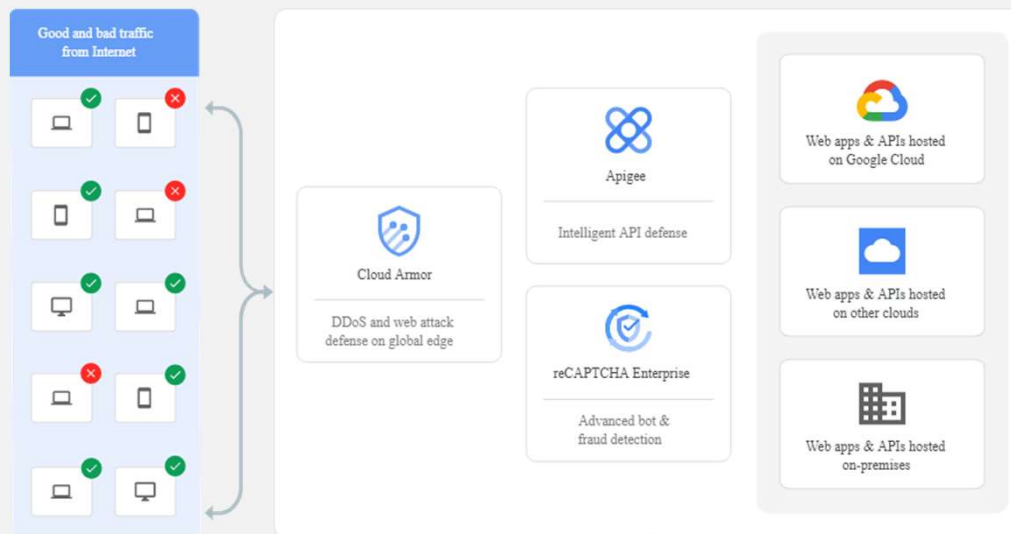
2. Requerimientos

3. Vulnerabilidades

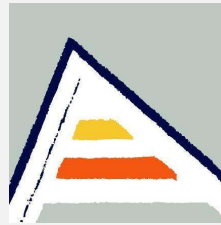
4. Ataques

5. PaaS

### Google Cloud Platform



MANAGED PROTECTION	STANDARD	PLUS (VERSIÓN BETA)	NOTAS
Facturación	Pago por uso	A partir de 3000 USD al mes	-
Recursos protegidos	Ninguno	Incluye los 100 primeros (a partir de ahí, cada recurso protegido adicional cuesta 30 USD al mes)	Los recursos protegidos engloban tanto los servicios de backend como los segmentos de backend
Reglas	1 USD al mes	Incluidas en la suscripción	-
Política	5 USD al mes	Incluida en la suscripción	-
Solicitudes	0,75 USD por cada millón de consultas	Incluidas en la suscripción	-
Tarifa por tratamiento de datos	Ninguno	<a href="#">Más información</a>	Activo a partir del momento de disponibilidad general
Periodo de vigencia	Ninguno	1 año	-



Grado en Ingeniería Informática

Sistemas distribuidos

# Seguridad en sistemas distribuidos

Víctor Vives

[vvives@dtic.ua.es](mailto:vvives@dtic.ua.es)

Departamento de Tecnología Informática y Computación

2021 - 2022