

Istio mTLS eks

Last updated by | Bibiana Alejandra Arismendi Mallama | 24 de jul de 2024 at 2:59 p. m. COT

⚠ Importante:

Todos los namespaces en el entorno de EKS de Bancolombia deben tener habilitado el sidecard de istio (istio-injection=enabled). Existen casos muy puntuales para productos de caja negra que no soportan integración con un serviceMesh, en ese caso se debe seguir el siguiente [proceso para solicitar la excepción](#).

Contents

- [Istio](#)
 - [GENERALIDADES](#)
 - [Introducción a Istio](#)
 - [¿Qué es un service mesh?](#)
 - [¿Qué es istio?](#)
 - [LINEAMIENTOS Y MEJORES PRÁCTICAS](#)
 - [CASOS DE USO](#)
 - [Arquitectura de istio en Bancolombia](#)
 - [¿CÓMO USAR EL SERVICIO EN BANCOLOMBIA?](#)
 - [Sidecar Istio](#)
 - [¿Qué es mTLS?](#)
 - [Recurso PeerAuthentication](#)
 - [¿Sobre la latencia?](#)
 - [¿Comunicación entre namespaces?](#)
 - [Ejemplo de laboratorios con mTLS y tráfico cifrado](#)
 - [CONTROLES DE SEGURIDAD](#)
 - [ENLACES DE INTERES](#)
 - [CONTROL DE VERSIONES](#)

Istio

GENERALIDADES

Introducción a Istio

¿Qué es un service mesh?

Un service mesh es una capa de infraestructura dedicada que puede agregar a sus aplicaciones. Le permite agregar de forma transparente capacidades como la observabilidad, la gestión del tráfico y la seguridad, sin agregarlas a su propio código. El término "malla de servicio" describe tanto el tipo de software que utiliza para implementar este patrón como el dominio de red o seguridad que se crea cuando utiliza ese software.

¿Qué es istio?

Istio es una red de servicios de código abierto que se superpone de forma transparente a las aplicaciones distribuidas existentes. Las potentes funciones de Istio brindan una forma uniforme y más eficiente de proteger, conectar y monitorear los servicios. Istio es el camino hacia el equilibrio de carga, la autenticación de servicio a servicio y la supervisión, con pocos o ningún cambio de código de servicio. Su poderoso plano de control trae características vitales, que incluyen:

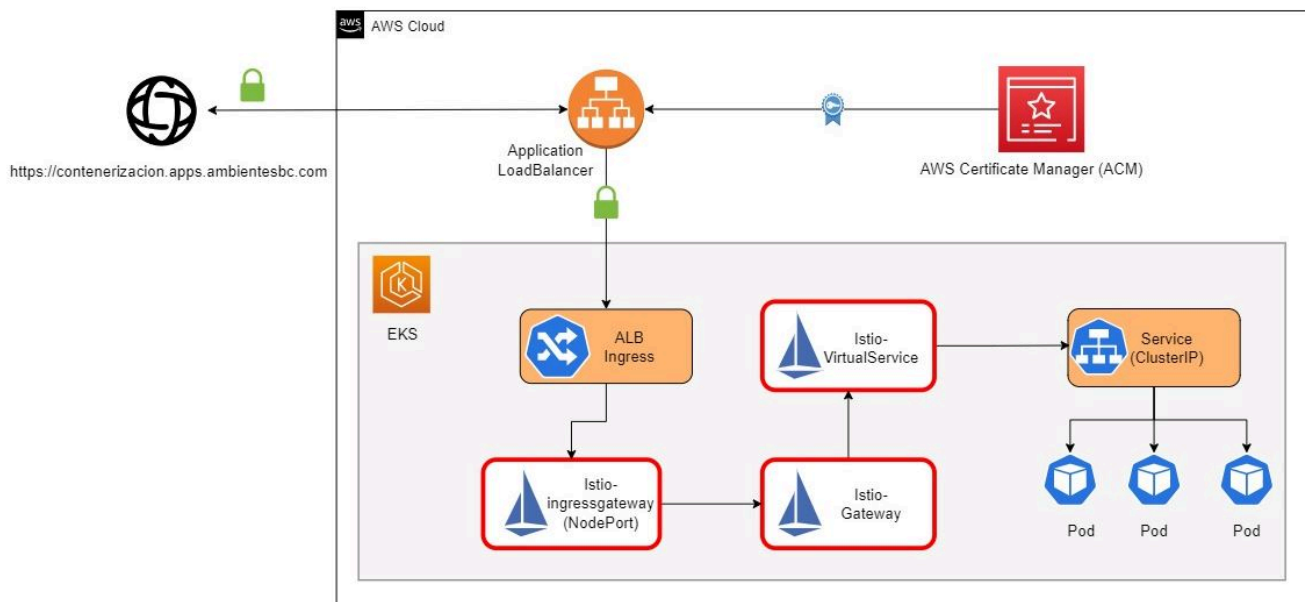
Fuente de consulta

LINEAMIENTOS Y MEJORES PRÁCTICAS

- Todos los recursos en istio deben estar etiquetados de acuerdo con [Estándar de etiquetas de recursos AWS](#)
- Un Virtual Service siempre va asociado a un Gateway
- La definición del paths del proyecto en el Gateway queda a disposición del proyecto si se hace de manera absoluta o relativa

CASOS DE USO

Arquitectura de istio en Bancolombia



¿CÓMO USAR EL SERVICIO EN BANCOLOMBIA?

Para el uso de istio se deben desplegar los recursos gateway, virtual service, destination rule (es opcional) puede hacer uso de istio y sus componentes para canary.



```

apiVersion: networking.istio.io/v1alpha3
kind: Gateway
metadata:
  name: #{app-gateway}#
  namespace: #{namespace}#
  labels:
    app.bancolombia.com.co/env: #{env}#
    app.bancolombia.com.co/cost-center: #{cost-center}#
    app.bancolombia.com.co/application-code: #{application-code}#
    app.bancolombia.com.co/project: #{project-name}#
    app.bancolombia.com.co/pmo: #{pmo}#
spec:
  selector:
    istio: ingressgateway # use istio default controller
  servers:
    - port:
        number: #{service-port}#
        name: #{service}#-port
        protocol: #{app-gateway-protocol}#
      hosts:
        - '#{gateway-internal-host}#'
---
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: #{service}#-vs
  namespace: #{namespace}#
  labels:
    app.bancolombia.com.co/env: #{env}#
    app.bancolombia.com.co/cost-center: #{cost-center}#
    app.bancolombia.com.co/application-code: #{application-code}#
    app.bancolombia.com.co/project: #{project-name}#
    app.bancolombia.com.co/pmo: #{pmo}#
spec:
  hosts:
    - '#{gateway-internal-host}#'
  gateways:
    - #{app-gateway}#
  http:
    - match:
        - uri:
            prefix: '#{path-prefix}#'
      rewrite:
        uri: '#{path-rewrite}#'
      route:
        - destination:
            host: #{service}#
            port:
              number: #{service-port}#

```

Sidecar Istio

El sidecar de istio es un contenedor adicional que sirve para abstraer métricas de su contenedor principal y aprovechar otras funcionalidades sin afectar su aplicación.

Para hacer uso de este sidecar debe cumplir una única regla:

- El namespace debe tener asignado el siguiente label `istio-injection=enabled`

Verá reflejado en el campo de READY 2/2 esto quiere decir que existen dos contenedores dentro de un pod, véalo gráficamente.

```

neytor@MacBook-Pro-de-Yonier git-bco % kubectl describe ns default
Name:      default
Labels:    istio-injection=enabled
           kubernetes.io/metadata.name=default
Annotations: <none>
Status:    Active

No resource quota.

No LimitRange resource.
neytor@MacBook-Pro-de-Yonier git-bco % kubectl get pods
NAME                                READY   STATUS    RESTARTS   AGE
skillfullers-validator-dp-59bcb4479c-j246b  2/2     Running   0           13h
neytor@MacBook-Pro-de-Yonier git-bco % kubectl get pods -o=jsonpath="{.items[*].spec.containers[*].name}"
skillfullers-validator istio-proxy%
neytor@MacBook-Pro-de-Yonier git-bco % █

```

Nota: Existe un pipeline operativo donde puede activar o desactivar a demanda istio-injection, una vez hecho esto debe reiniciar los pods, [Enlace pipeline documentación](#)

¿Qué es mTLS?

mTLS (mutual Transport Layer Security) en Istio se refiere a la autenticación y el cifrado basado en certificados para la comunicación segura entre servicios dentro de un entorno de microservicios gestionado por Istio.

mTLS implica el uso de certificados TLS tanto en el lado del cliente como en el lado del servidor para establecer una comunicación segura y autenticada entre los servicios. Cada servicio tiene su propio certificado y clave privada, y se establece una confianza mutua entre los servicios mediante el intercambio y la validación de certificados (el sidecar de istio se encarga de esto).

CA interna de Istio: Istio también proporciona su propio sistema de CA interna, conocido como Istio Citadel, que puede ser utilizado para la administración de certificados.

IMPORTANTE: El envoy o sidecar es quien facilita la comunicación entre microservicios de manera segura.

Recurso PeerAuthentication

PeerAuthentication define cómo se tunelizará (o no) el tráfico al sidecar.

¿Cuáles son los modos existentes?

Nombre	Descripción
UNSET	Heredar del padre, si tiene uno. De lo contrario, se tratará como PERMISIVO.
DISABLE	La conexión no tiene un túnel
PERMISSIVE	La conexión puede ser texto plano o túnel mTLS.
STRICT	La conexión es un túnel mTLS (se debe presentar TLS con certificado).

Para nuestro caso únicamente usaremos el modo STRICT debido a que si se configura en PERMISSIVE tendríamos el mismo problema "comunicaciones sin cifrar"

Habilitar mTLS

Para habilitar mTLS solo se debe aplicar este manifiesto en el namespace de istio-system y quedará de manera global en el cluster.

```
apiVersion: security.istio.io/v1beta1
kind: PeerAuthentication
metadata:
  name: mtls-global
  namespace: istio-system
spec:
  mtls:
    mode: STRICT
```



¿Sobre la latencia?

Por defecto cuando la comunicación entra por el balanceador la toma istio y es cifrada, por ende no agregaría una latencia que sea evidente una vez aplicado el mTLS

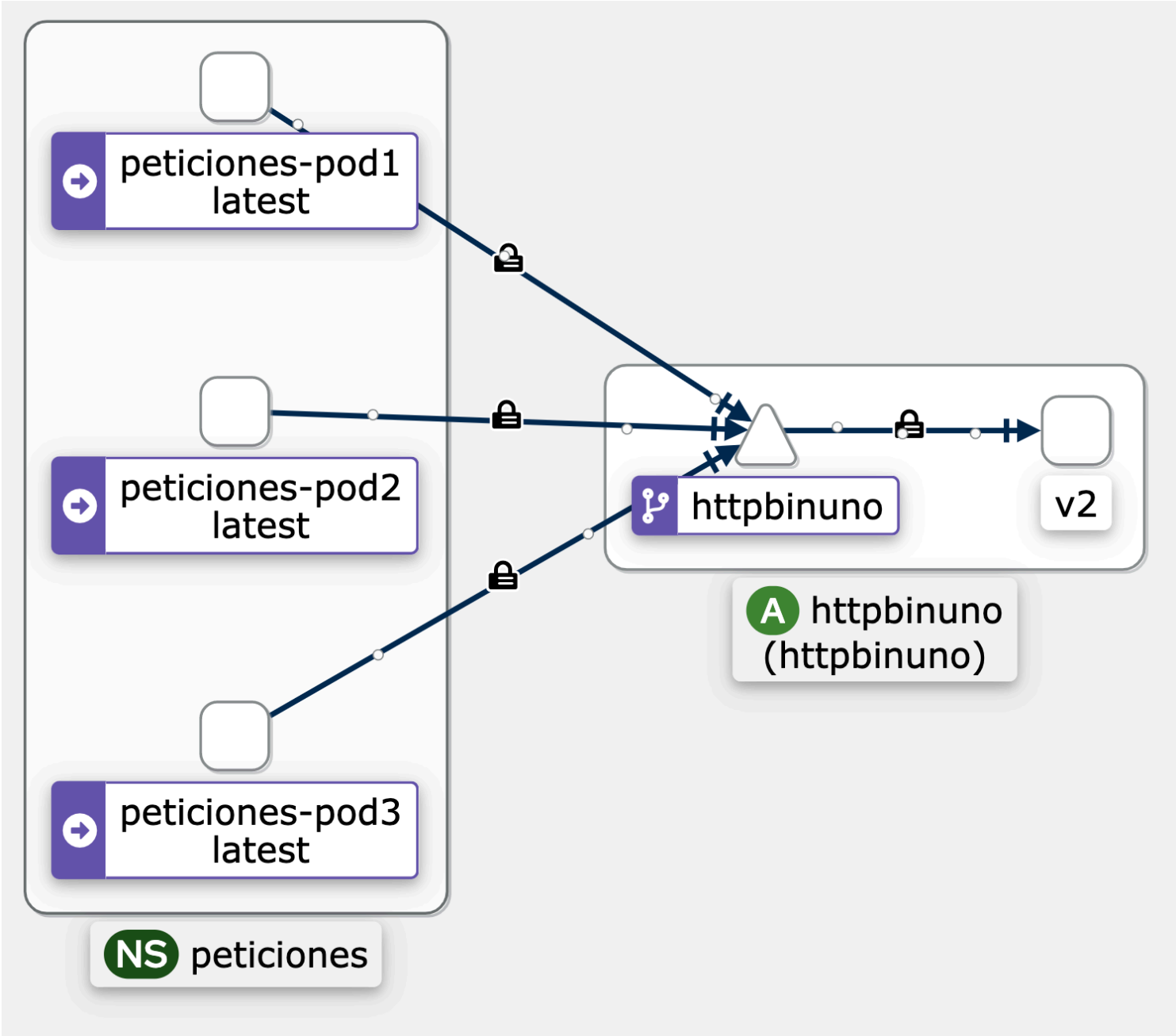
¿Comunicación entre namespaces?

Cuando se quiere comunicar el namespace A con el namespace B y se tiene mTLS habilitado es una comunicación segura que implica el uso de certificados de ambos lados (para el ejemplo namespace A y B), el hecho de cifrar y descifrar los mensajes puede agregar latencia a las aplicaciones con este modo de comunicación.

IMPORTANTE: Es de aclarar que desde arquitectura las comunicaciones se deben dar a través del balanceador de carga, por ende no existiría dicha latencia, se tiene configurado el recurso NETWORK POLICY en todos los namespaces que impiden la comunicación directa entre namespace A y B para el ejemplo.

Ejemplo de laboratorios con mTLS y tráfico cifrado

Gráfica



Overview Traffic Inbound Metrics Traces

Inbound Traffic

Status ↑	Name ↓	Rate ↓	Percent Success ↓	Protocol ↓	Actions
🔍	🔍 W peticiones-pod1	635.44rps	100.0%	TCP 🔒	View metrics
🔍	🔍 W peticiones-pod3	677.73rps	100.0%	TCP 🔒	View metrics
🔍	🔍 W peticiones-pod2	665.00rps	100.0%	TCP 🔒	View metrics

Outbound Traffic

Status ↑	Name ↓	Rate ↓	Percent Success ↓	100 % of mTLS traffic	Actions
🔍	🔍 W httpbinuno	1978.18rps	100.0%	TCP 🔒	View metrics

No.	Time	Source	Destination	Protocol	Length	Info
581	12.092407	100.67.44.218	100.67.44.179	TCP	74	33108 → 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM TSval=2948427817 TSecr=0 WS=128
582	12.092435	100.67.44.179	100.67.44.218	TCP	74	80 → 33108 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=2345255053 TSecr=2948427817 WS=128
583	12.092440	100.67.44.218	100.67.44.179	TCP	66	33108 → 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=2948427817 TSecr=2345255053
584	12.092539	100.67.44.218	100.67.44.179	TCP	2261	33108 → 80 [PSH, ACK] Seq=1 Ack=1 Win=62848 Len=2195 TSval=2948427817 TSecr=2345255053
585	12.092553	100.67.44.179	100.67.44.218	TCP	66	80 → 33108 [ACK] Seq=1 Ack=2196 Win=60544 Len=0 TSval=2345255053 TSecr=2948427817
586	12.092917	100.67.44.179	100.67.44.218	TCP	295	80 → 33108 [PSH, ACK] Seq=1 Ack=2196 Win=60544 Len=229 TSval=2345255053 TSecr=2948427817
587	12.092921	100.67.44.218	100.67.44.179	TCP	66	33108 → 80 [ACK] Seq=2196 Ack=230 Win=62720 Len=0 TSval=2948427817 TSecr=2345255053
588	12.093148	100.67.44.218	100.67.44.179	TCP	130	33108 → 80 [PSH, ACK] Seq=2196 Ack=230 Win=62720 Len=64 TSval=2948427817 TSecr=2345255053
589	12.093255	100.67.44.218	100.67.44.179	TCP	1096	33108 → 80 [PSH, ACK] Seq=2260 Ack=230 Win=62720 Len=1030 TSval=2948427817 TSecr=2345255053
590	12.093278	100.67.44.179	100.67.44.218	TCP	66	80 → 33108 [ACK] Seq=230 Ack=3290 Win=59520 Len=0 TSval=2345255053 TSecr=2948427817
591	12.093348	100.67.44.179	100.67.44.218	TCP	4691	80 → 33108 [PSH, ACK] Seq=230 Ack=3290 Win=59520 Len=4625 TSval=2345255053 TSecr=2948427817
592	12.094394	100.67.44.179	100.67.44.218	TCP	318	80 → 33108 [PSH, ACK] Seq=4855 Ack=3290 Win=59520 Len=252 TSval=2345255053 TSecr=2948427817
593	12.094406	100.67.44.218	100.67.44.179	TCP	66	33108 → 80 [ACK] Seq=3290 Ack=5107 Win=57856 Len=0 TSval=2948427819 TSecr=2345255054
594	12.094414	100.67.44.179	100.67.44.218	TCP	521	80 → 33108 [PSH, ACK] Seq=5107 Ack=3290 Win=59520 Len=455 TSval=2345255055 TSecr=2948427817
595	12.094591	100.67.44.218	100.67.44.179	TCP	90	33108 → 80 [PSH, ACK] Seq=3290 Ack=5562 Win=57472 Len=24 TSval=2948427819 TSecr=2345255055
596	12.094704	100.67.44.179	100.67.44.218	TCP	90	80 → 33108 [PSH, ACK] Seq=5562 Ack=3314 Win=59520 Len=24 TSval=2345255055 TSecr=2948427819
597	12.094718	100.67.44.179	100.67.44.218	TCP	66	80 → 33108 [FIN, ACK] Seq=5586 Ack=3314 Win=59520 Len=0 TSval=2345255055 TSecr=2948427819
598	12.094725	100.67.44.218	100.67.44.179	TCP	66	33108 → 80 [FIN, ACK] Seq=3314 Ack=5587 Win=57472 Len=0 TSval=2948427819 TSecr=2345255055
599	12.094738	100.67.44.179	100.67.44.218	TCP	66	80 → 33108 [ACK] Seq=5587 Ack=3315 Win=59520 Len=0 TSval=2345255055 TSecr=2948427819
600	12.661589	10.124.97.210	100.67.44.218	TCP	74	36490 → 15021 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM TSval=1207948560 TSecr=0 WS=128
601	12.661601	100.67.44.218	10.124.97.210	TCP	74	15021 → 36490 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=4046289004 TSecr=1207948560 WS=128
602	12.661609	10.124.97.210	100.67.44.218	TCP	66	36490 → 15021 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=1207948560 TSecr=4046289004
603	12.661671	10.124.97.210	100.67.44.218	HTTP	186	GET /healthz/ready HTTP/1.1
604	12.661674	100.67.44.218	10.124.97.210	TCP	66	15021 → 36490 [ACK] Seq=1 Ack=121 Win=62592 Len=0 TSval=4046289004 TSecr=1207948560
> Frame 592: 318 bytes on wire (2544 bits), 318 bytes captured (2544 bits)						0000 9a e4 bb 2e 43 48 9a 46 29 52 5d 52 08 00 45 00 ...CH.F)R]R -E
> Ethernet II, Src: 9a:46:29:52:5d:52 (9a:46:29:52:5d:52), Dst: 9a:e4:bb:2e:43:48 (9a:e4:bb:2e:43:48)						0010 01 30 5d cb 40 00 fe 06 fb e8 64 43 2c b3 64 43 ...0] @...dC, dC
> Internet Protocol Version 4, Src: 100.67.44.179, Dst: 100.67.44.218						0020 2c da 00 50 81 54 c7 95 b3 ea 37 e0 4f 6a 80 18 ...P T...7.0]..
> Transmission Control Protocol, Src Port: 80, Dst Port: 33108, Seq: 4855, Ack: 3290, Len: 252						0030 01 d1 23 36 00 00 01 01 08 0a 8b c9 c0 8f af bd ...#6... ..
						0040 70 29 17 03 03 00 07 aa 1b 50 cc 1e 03 62 10 a3 p).....P...b..
						0050 ff 07 5a d3 e9 3f f0 13 89 5b d3 da 9d cc c5 d4 ...Z...?...[.....
						0060 1d d5 37 40 1d ed e2 03 71 b3 45 37 60 14 3d 03 ...7@... q'E`'=.
						0070 8e 15 7b 8b 6d e3 c8 cf bd c6 84 86 80 35 74 c4 ...{m...3...5t...
						0080 d5 7a c2 aa 38 76 61 d6 c3 c8 33 a0 c2 de bf 08 ...z..8va... ..
						0090 6e 89 48 c2 c6 c6 11 fb cd 66 10 a1 e9 4f 12 da n.H... ..f...0...
						00a0 af c3 da 24 30 5e ab 8a 3a e9 4f dc e7 d7 97 cd ...,\$0^...:0.....
						00b0 91 2c 3d 48 06 e0 b1 ca 6d 25 83 0b b0 8f c4 87 ...=H...m%... ..
						00c0 4f 15 92 8b a7 79 0f cd 7f 2f ea 40 65 fb aa ab 0...y...? /@e... ..
						00d0 79 cf a3 95 bb be a9 3f a0 c0 b9 07 54 9a d2 b0 y.....?T... ..
						00e0 6a 4b cf f6 c4 8c 17 68 de d2 9c 70 f3 57 a3 18 jK... ..h...p.W... ..
						00f0 13 17 55 d3 bc 1c da bc ca df e7 41 75 bc 02 1e ...U... ..Au... ..
						0100 80 d1 03 8c 5c 4d ab b7 48 c6 82 69 35 46 6a 97 ...~MKK..H...15Fj...
						0110 bc 9d ff 30 0c 00 ad 28 bc de f7 6e b6 f5 ca 94 ...0... (..N.n... ..
						0120 b3 16 99 94 24 17 b1 26 ac 01 2a a3 98 d7 dc 1a ...\$.&.*.....
						0130 d7 60 b7 35 f6 a1 86 3c 74 39 cb 55 2a f5 ...5...< t9.U*..

CONTROLES DE SEGURIDAD

Para mayor informacion sobre los controles de seguridad aplicables a este servicio, consulte [CODI](#)

Si tiene problemas para acceder a la herramienta CODI, por favor consulte el siguiente [enlace](#)

ENLACES DE INTERES

- [Istio](#)
- [PeerAuthentication](#)
- [mTLS](#)
- [Acuerdos de nivel de serivcios \(SLA\)](#)

CONTROL DE VERSIONES

Fecha	Descripción	Realizó	Aprobó
2022/10/20	Versión inicial	@Yonier Manuel Asprilla Gomez @Mauricio Bohorquez Orozco	
2023/10/10	Istio mTLS	@Yonier Manuel Asprilla Gomez	