

EL ENTORNO DE EJECUCIÓN PARA LA ERA HUMANA

Donde los datos, la IA, las aplicaciones, las comunicaciones y la autoridad operan de forma segura dentro de límites definidos por las personas.

LA TESIS GENERAL

AttesTorr proporciona Layer ZERO: un entorno de ejecución gobernado en el que la actividad digital se admite, delimita, ejecuta y cierra, y puede evaluarse de manera independiente antes de que pueda existir una autoridad sucesora. La seguridad no se coloca simplemente alrededor de la ejecución. Se expresa mediante las condiciones bajo las cuales se permite que existan la ejecución y la autoridad.

Fausto Aceves | AttesTorr, Inc.

Documento técnico de arquitectura para difusión pública | Octubre de 2026 | No confidencial

Estado de desarrollo: arquitectura completa; implementación de referencia en curso; previo al producto mínimo viable (MVP); sin ingresos.

TESIS EJECUTIVA

El mundo digital ha acumulado aplicaciones potentes, redes, infraestructura en la nube, controles de ciberseguridad, sistemas de comunicaciones e IA cada vez más autónoma. Lo que no ha estandarizado es el límite de ejecución que determina cuándo comienza la autoridad, a qué puede acceder, qué puede hacer, cuánto tiempo puede existir y qué debe ocurrir cuando finaliza el trabajo.

AttesTorr aborda esa capa ausente. Layer ZERO convierte la ejecución declarada en la unidad de control. Las personas y las organizaciones definen el límite permitido; el entorno vincula la identidad, la autoridad, los datos, las aplicaciones, las comunicaciones, los destinos, los efectos, el tiempo y las condiciones de cierre a esa ejecución.

El resultado es una propuesta sencilla: los sistemas digitales potentes no deberían necesitar confianza permanente ni autoridad continua simplemente porque están conectados. Deberían operar dentro de un límite cuya admisión, aplicación, finalización y evaluación sean posibles.

LÍMITES DEFINIDOS POR PERSONAS

Las personas y las instituciones determinan el propósito, los permisos, las políticas y los resultados aceptables.

EJECUCIÓN SEGURA

La identidad, la autoridad, los datos, las herramientas, las rutas, los efectos y la duración quedan delimitados a la ejecución declarada.

CIERRE DISEÑADO

La identidad y la autoridad de la ejecución original terminan en CLOSE; el estado de trabajo protegido se maneja conforme a reglas de desmantelamiento declaradas.

SUCESOR NUEVO

Lo que viene después requiere una nueva admisión y autoridad recién emitida. Las pruebas pueden sobrevivir; la autoridad, no.

1 | DE LA SEGURIDAD ALREDEDOR DE LOS SISTEMAS A LA SEGURIDAD EN LA EJECUCIÓN

La ciberseguridad convencional sigue siendo esencial: los sistemas de identidad, el cifrado, los controles de dispositivos finales, la segmentación de redes, la confianza cero, la supervisión, la gestión de vulnerabilidades y la respuesta a incidentes abordan riesgos reales. Sin embargo, muchos de esos controles protegen sistemas en los que las credenciales, sesiones, integraciones, rutas de datos y privilegios pueden seguir disponibles después de la tarea inmediata.

Layer ZERO complementa dichos controles al gobernar la duración de la propia autoridad de ejecución. La pregunta arquitectónica pasa a ser no solo «¿puede conectarse este usuario o máquina?», sino también «¿está autorizada esta ejecución, en este momento, a producir este efecto, sobre estos datos, por esta ruta, para este propósito y durante este período?».

Por tanto, la seguridad pasa a formar parte del contrato de ejecución. Una identidad válida no equivale a autoridad ilimitada. La conectividad no es permiso. Una salida del modelo no es autorización. Una admisión anterior no implica automáticamente la admisión del sucesor.

2 | QUÉ OPERA DENTRO DEL ENTORNO

DATOS — Los mensajes, documentos, registros, imágenes, audio, video, información de sensores, instrucciones, respuestas, estado de trabajo y otros contenidos digitales compatibles pueden gobernarse según condiciones declaradas de alcance, persistencia y exportación.

APLICACIONES — Las aplicaciones privadas o empresariales se convierten en interfaces controladas hacia las capacidades. Una aplicación recibe únicamente la autoridad, los datos, los destinos y los efectos permitidos para la ejecución.

COMUNICACIONES — Las comunicaciones entre personas, entre personas y máquinas, y entre máquinas pueden operar bajo el mismo límite de ejecución, en lugar de tratarse como un universo de confianza separado.

IA — Los modelos y agentes pueden analizar, proponer, comunicarse y solicitar efectos sin recibir automáticamente credenciales del entorno ni autoridad permanente.

AUTORIDAD — La autoridad es explícita, limitada en alcance y tiempo, y vinculada a la ejecución. El derecho a actuar es distinto de la identidad y de la posesión de datos.

SEGURIDAD — El entorno restringe las condiciones bajo las cuales puede continuar la ejecución protegida y exige un comportamiento de cierre definido cuando esas condiciones terminan o fallan.

PERSONA / ORGANIZACIÓN → define propósito, política, permisos y resultados aceptables → LAYER ZERO → DATOS • APLICACIONES • COMUNICACIONES • IA • AUTORIDAD

Ejecución delimitada → cierre diseñado → evidencia evaluable de forma independiente → nuevo sucesor.

3 | EL CICLO DE VIDA DE LAYER ZERO

ADMIT → BIND → EXECUTE → CLOSE → SUCCESSOR

ADMIT (ADMITIR) — Determinar si la ejecución propuesta está autorizada para comenzar conforme a la identidad, política, aprobaciones, entorno, objetivos y requisitos de aseguramiento actuales.

BIND (VINCULAR) — Crear una identidad nueva y limitada a la ejecución, y vincular el propósito, autoridad, datos, aplicaciones, herramientas, rutas de red, destinos, contexto criptográfico, efectos y duración permitidos.

EXECUTE (EJECUTAR) — Permitir el trabajo únicamente dentro del alcance vinculado en los puntos de aplicación correspondientes. La autoridad nueva no se infiere de la conectividad, el acceso anterior ni la intención del modelo.

CLOSE (CERRAR) — Terminar el contexto de ejecución y la autoridad originaria, manejar el estado de trabajo protegido según las reglas de desmantelamiento declaradas y completar la evidencia canónica exigida.

SUCCESSOR (SUCESOR) — Exigir una admisión nueva, una vinculación nueva y autoridad recién emitida. Un sucesor no hereda la ejecución originaria solo porque subsistan salidas permitidas o pruebas.

4 | CONTROL HUMANO SIN CUELLOS DE BOTELLA HUMANOS

«Límites definidos por las personas» no significa que una persona deba aprobar manualmente cada instrucción de la máquina. Significa que el alcance legítimo procede de políticas humanas o institucionales y se traduce en condiciones aplicables durante la ejecución. La automatización puede avanzar a velocidad de máquina dentro de esas condiciones sin ampliarlas silenciosamente.

Esto mantiene una distinción importante: la identidad puede persistir mientras la autoridad sigue siendo efímera. Una persona puede continuar siendo empleada, cliente, profesional de la salud, analista, administradora o ciudadana, mientras cada ejecución con consecuencias recibe únicamente la autoridad adecuada para ese momento y propósito.

HECHO INSTITUCIONAL PERSISTENTE | HECHO LIMITADO A LA EJECUCIÓN

Identidad humana o de máquina | Autoridad de ejecución actual

Relación laboral o de otro tipo | Tarea y propósito permitidos

Política de la organización | Datos, aplicaciones, herramientas y efectos permitidos

Propiedad de la infraestructura | Contexto criptográfico o de sesión actual

Responsabilidad a largo plazo | Duración delimitada y condiciones de cierre

5 | APLICACIONES Y COMUNICACIONES PRIVADAS

El entorno puede presentar aplicaciones de propiedad de la organización o del cliente como puertas controladas hacia capacidades permitidas. Los usuarios no necesitan acceso generalizado a la infraestructura subyacente solo para realizar trabajo autorizado. La aplicación es una interfaz; Layer ZERO gobierna la autoridad de ejecución que existe detrás de ella.

La mensajería es un ejemplo, no el límite. El mismo modelo puede gobernar comunicaciones, documentos, flujos de trabajo, interacciones con IA, bases de datos, procesamiento de sensores y otras

actividades compatibles de procesamiento de datos. Cambia el contenido; no cambia el requisito de ejecución delimitada.

Esto crea un entorno coherente en el que las comunicaciones y la computación pueden compartir los mismos principios de identidad, autoridad, alcance, persistencia, exportación, cierre y admisión del sucesor.

6 | LA CIBERSEGURIDAD COMO CONSECUENCIA DELIMITADA

Ninguna arquitectura elimina el riesgo cibernético. La tesis de seguridad de AttesTorr consiste en reducir aquello a lo que una intrusión exitosa puede acceder legítimamente, lo que puede hacer, retener o trasladar al futuro. El objetivo no es afirmar que una intrusión sea imposible. Es impedir que una intrusión fabrique una autoridad que nunca se concedió y terminar la autoridad originaria cuando termina la ejecución.

Esto plantea tres preguntas distintas de contención:

- Radio de impacto de los datos — ¿a qué información protegida puede acceder esta ejecución o qué información puede retener?
- Radio de impacto de los efectos — ¿qué acciones puede provocar esta ejecución en el mundo o en los sistemas conectados?
- Radio de impacto de la autoridad — ¿qué facultades legítimas puede ejercer esta ejecución y durante cuánto tiempo?

El objetivo arquitectónico es: DATOS DELIMITADOS → EFECTOS DELIMITADOS → AUTORIDAD DELIMITADA → CONSECUENCIAS DELIMITADAS.

7 | SOBERANÍA DEL CLIENTE

AttesTorr está diseñado para que el cliente pueda ser propietario del entorno en el que ocurre la ejecución: infraestructura, aplicaciones, datos, claves, identidades, políticas de autorización y lógica de negocio. Layer ZERO gobierna cuándo existe autoridad de ejecución dentro de ese entorno y cómo se delimita y termina esa autoridad.

Esto resulta especialmente importante para empresas, instituciones reguladas, gobiernos, salud, finanzas, sistemas industriales y otros entornos en los que puede ser inaceptable externalizar el control de datos sensibles o de la autoridad principal.

EL CLIENTE DEFINE / POSEE | LAYER ZERO GOBIERNA

Infraestructura y límite de despliegue | Admisión y ciclo de vida de ejecución

Aplicaciones y lógica de negocio | Identidad y autoridad limitadas a la ejecución

Datos y persistencia permitida | Alcance y efectos delimitados en tiempo de ejecución

Claves y sistemas de identidad | Requisitos de cierre e invalidación de autoridad

Política de autorización | Requisitos de evidencia y disciplina del sucesor

8 | QUÉ ES LAYER ZERO Y QUÉ NO ES

Layer ZERO es la capa fundamental de ejecución donde la ejecución se admite, delimita, gobierna y cierra, y se hace evaluable de manera independiente antes de que operen las capas superiores. Puede situarse debajo de la IA, las aplicaciones, las comunicaciones, los flujos de trabajo y otras actividades digitales.

No supone que la ciberseguridad, la identidad, las redes, la criptografía, la gobernanza o los controles de infraestructura existentes se vuelvan innecesarios. Esos sistemas siguen formando parte de la defensa en profundidad. Layer ZERO aborda un problema arquitectónico diferente: la existencia y duración de la autoridad de ejecución.

Tampoco afirma una eliminación universal. El aseguramiento se limita al perímetro declarado, los controles implementados, la evidencia y el perfil de verificación. Las salidas permitidas y la evidencia canónica pueden sobrevivir a CLOSE sin conservar la Sala originaria ni su autoridad.

9 | LA TESIS DE LA ERA HUMANA

La era industrial organizó la producción física. La era de internet conectó la información. La era de la nube hizo elástica la computación. La era de la IA está haciendo que las capacidades de las máquinas sean cada vez más autónomas y trascendentes.

La era humana requiere algo diferente: una manera de permitir actuar a los sistemas digitales potentes sin que las personas tengan que ceder el control permanente de sus datos, identidad, aplicaciones, comunicaciones o autoridad.

La propuesta de AttesTorr es que el límite debe ser arquitectónico, no aspiracional. La intención humana y las políticas institucionales deben convertirse en condiciones de ejecución aplicables. La autoridad debe tener un comienzo, un alcance, una duración y un final.

EL ENTORNO DE EJECUCIÓN PARA LA ERA HUMANA

Donde los datos, la IA, las aplicaciones, las comunicaciones y la autoridad operan de forma segura dentro de límites definidos por las personas.

Límites definidos por personas. Ejecución segura. Sin autoridad permanente.

ESTADO DE DESARROLLO Y ASEGURAMIENTO

AttesTorr describe su arquitectura como completa, con implementación de referencia en curso, antes del MVP y sin ingresos. Este documento describe requisitos arquitectónicos y propiedades previstas, no una evaluación de seguridad independiente completada ni un despliegue en producción. El aseguramiento real depende del plano de aplicación implementado, el límite de confianza declarado, la semántica de la evidencia, la configuración del despliegue y la verificación independiente. Las afirmaciones de rendimiento, incluida la latencia del desmantelamiento, requieren validación bajo condiciones de referencia definidas antes de presentarse como garantías de producción.

CONTINUIDAD ARQUITECTÓNICA

Este documento es una capa de posicionamiento general sobre la arquitectura establecida de AttesTorr. No introduce una fase nueva de ejecución ni eleva un nuevo elemento primitivo. El ciclo de vida de ejecución sigue siendo ADMIT → BIND → EXECUTE → CLOSE → SUCCESSOR. La verificación independiente ocurre después de CLOSE y no constituye una sexta fase de ejecución.