

MINIMIZAR EL MUNDO ATACABLE

Ejecución efímera, autoridad temporal y la próxima frontera de la ciberseguridad

Documento técnico de ciberseguridad | Octubre de 2026

AttesTorr, Inc. | Concepto y arquitectura Layer ZERO

EL PRINCIPIO DE ATTESTORR

Minimizar lo que puede ser atacado.

Minimizar durante cuánto tiempo puede ser atacado.

Minimizar lo que permanece después de que se cierra la ventana de ataque.

Menos persistencia. Menos exposición. Menos oportunidades.

RESUMEN EJECUTIVO

La ciberseguridad ha dedicado décadas a hacer que los sistemas persistentes sean más difíciles de penetrar. Los cortafuegos protegen redes. El cifrado protege datos. Los sistemas de identidad protegen cuentas. La seguridad de terminales protege máquinas. La supervisión intenta identificar a los atacantes después de su llegada.

Todo ello sigue siendo necesario. Pero comparte una suposición de fondo: aquello que se protege continúa existiendo.

La mejor manera de reducir la superficie de ataque es reducir lo que existe para ser atacado.

AttesTorr Layer ZERO introduce entornos de ejecución en los que la autoridad, los datos de trabajo, las credenciales, identidades, claves, interacciones con IA y otros estados sensibles pueden limitarse a un propósito y una duración determinados.

Se admite una nueva Sala de Confianza Efímera (Ephemeral Trust Room), y la identidad y el propósito se vinculan a ella. La ejecución gobernada sucede dentro de un límite de confianza declarado. Nada sale únicamente porque una aplicación lo considere permitido: cualquier exportación debe satisfacer sus condiciones de autorización después de cerrarse la sala. En el cierre se invalidan la autoridad y la identidad limitadas a la ejecución. Las pruebas pueden permanecer para verificación independiente sin exigir que continúe existiendo el entorno de ejecución sensible.

REDUCCIÓN DE SUPERFICIE DE ATAQUE — Hay menos estado persistente disponible como objetivo.

REDUCCIÓN DE VENTANA DE ATAQUE — El estado sensible y la autoridad están disponibles durante menos tiempo.

El objetivo no es afirmar que un sistema jamás pueda ser atacado. Es dar al atacante menos elementos que atacar, menos tiempo para atacarlos, menos autoridad que robar y menos estado útil que recuperar después.

La afirmación verificable es más limitada que la desaparición. AttesTorr está diseñado para que pueda verificarse de forma independiente que la autoridad y la identidad limitadas a la ejecución terminaron y que no existe una vía admisible para continuarlas dentro del límite de confianza declarado. No afirma demostrar que todas las copias de datos sensibles hayan dejado de existir ni controlar copias fuera de dicho límite. Reducir lo que persiste disminuye la exposición; no es por sí solo una garantía.

PANORAMA DE LA ARQUITECTURA

ADMIT → BIND → EXECUTE → CLOSE → SUCCESSOR

La verificación independiente evalúa la evidencia de cierre después de CLOSE. No es una fase del ciclo de vida.

Layer ZERO gobierna un ciclo de vida de ejecución delimitado en el que no se presupone la continuidad. Una ejecución posterior debe establecer su propia autoridad en vez de heredar silenciosamente la de la Sala de Confianza Efímera anterior.

1. EL PROBLEMA DE LA PERSISTENCIA

La computación moderna se construyó alrededor de la persistencia. Las aplicaciones conservan estado. Los servidores acumulan datos. Las credenciales siguen siendo válidas. Los registros se multiplican. Las cachés sobreviven. Las sesiones dejan artefactos. Las copias de seguridad reproducen información. Los sistemas biométricos pueden conservar información de identidad. Los sistemas de IA pueden generar todavía más copias, incrustaciones vectoriales, historiales, instrucciones, telemetría e información derivada.

Cada elemento persistente puede convertirse en parte del entorno atacable. Por tanto, la ciberseguridad tradicional afronta un problema creciente: cuanto más valiosa se vuelve la infraestructura digital, mayor es el conjunto de elementos que deben defenderse continuamente.

AttesTorr cambia la premisa. No todo lo que debe existir durante el cálculo tiene que seguir existiendo después.

2. CIBERSEGURIDAD MEDIANTE LA MINIMIZACIÓN DE LA EXISTENCIA

Minimizar lo que existe. Minimizar cuánto tiempo existe. Minimizar la autoridad que posee. Verificar que terminó.

El principio de AttesTorr cambia las preguntas que formula la seguridad.

En lugar de preguntar únicamente cómo defender los datos, Layer ZERO también pregunta si esos datos deben permanecer. En lugar de preguntar solo cómo proteger una credencial, pregunta si esa autoridad debe seguir siendo válida después de terminar la ejecución. En lugar de preguntar cómo proteger continuamente un entorno de ejecución, pregunta por qué ese entorno debería seguir existiendo.

La diferencia es fundamental.

3. LA SALA DE CONFIANZA EFÍMERA

ADMIT → BIND → EXECUTE → CLOSE → SUCCESSOR

La verificación independiente de las pruebas de cierre ocurre por separado, después de CLOSE.

PASO | FUNCIÓN

ADMIT (ADMITIR) — Una función de admisión designada determina si la persona, máquina, IA, aplicación, dispositivo, dato u otro participante puede entrar en la ejecución, y solo esa función emite la identidad de la ejecución. Llegar con información de entrada o una conexión no establece por sí solo autoridad.

BIND (VINCULAR) — Vincular identidad, propósito, autoridad, alcance y restricciones pertinentes a esa ejecución.

EXECUTE (EJECUTAR) — Realizar el trabajo autorizado dentro del límite declarado.

CLOSE (CERRAR) — Terminar el entorno de ejecución y la autoridad limitada a él conforme al perfil de cierre aplicable.

SUCCESSOR (SUCESOR) — Cuando se solicita una ejecución posterior, se comprueba la evidencia de cierre de la ejecución anterior y se admite por separado la nueva ejecución, con una identidad nueva. No se hereda autoridad activa de la anterior.

VERIFICACIÓN INDEPENDIENTE (FUERA DEL CICLO) — No es una fase del ciclo de vida. Después del cierre, un verificador independiente evalúa la evidencia completa de cierre y llega a su propia conclusión. No emite un certificado de finalidad, y su conclusión no concede autoridad a ninguna ejecución sucesora.

Una Sala de Confianza Efímera es un entorno de ejecución ligado a un propósito y creado para un ciclo de vida gobernado.

La propiedad esencial es que no se presupone continuidad. La siguiente ejecución debe obtener su propia autoridad.

4. REDUCIR LA SUPERFICIE DE ATAQUE

La naturaleza efímera cambia lo que puede encontrar un atacante. Un entorno persistente puede exponer credenciales de larga duración, información en caché, estado de aplicaciones, tokens de sesión, archivos temporales sensibles, historiales de IA, datos biométricos de trabajo, permisos permanentes, identidades de máquina, claves de cifrado, memoria residual, bases de datos, registros, telemetría, servicios abandonados y estados históricos de ejecución.

Una arquitectura efímera procura eliminar la persistencia innecesaria en estas categorías. Esto no elimina las vulnerabilidades durante la ejecución. Cambia lo que permanece disponible antes, durante y, especialmente, después de la ejecución.

Menos persistencia crea una menor superficie de ataque residual.

5. REDUCIR LA VENTANA DE ATAQUE

La superficie de ataque es solo una dimensión. El tiempo es otra.

Una credencial disponible durante un año presenta un riesgo distinto de una autoridad válida para una única ejecución. Un entorno que funciona continuamente ofrece una oportunidad diferente de otro que se cierra inmediatamente después de cumplir su propósito autorizado. Una sesión activa da tiempo al atacante para explorar. Una ejecución breve comprime esa oportunidad.

Por ello, AttesTorr trata el tiempo de cierre como una propiedad de seguridad. El objetivo es pasar rápidamente de la ejecución activa a un estado cerrado y seguro.

En implementaciones capaces de lograr un cierre seguro extremadamente rápido, la ventana de ataque utilizable puede aproximarse a la duración de la propia ejecución autorizada en vez de a la vida útil de la infraestructura subyacente.

Reducimos no solo la superficie de ataque. Reducimos el tiempo de ataque.

6. AUTORIDAD TEMPORAL

Los sistemas persistentes suelen acumular autoridad permanente. Los usuarios permanecen conectados. Las claves de API siguen siendo válidas. Las credenciales de máquina siguen disponibles. Los servicios conservan privilegios mucho después de finalizar una tarea específica. Los agentes de IA pueden recibir permisos más amplios o duraderos que los necesarios para el trabajo.

En cambio, AttesTorr admite autoridad limitada a la ejecución. Puede estar delimitada por propósito, identidad, tiempo y entorno, ser intransferible, revocable y extingible al cierre.

Cuando termina la ejecución gobernada, la autoridad correspondiente no necesita sobrevivir.

Un atacante no puede explotar indefinidamente una autoridad que ya no existe.

7. BIOMETRÍA SIN AUTORIDAD BIOMÉTRICA PERMANENTE

BIOMETRÍA → VERIFICAR → AUTORIDAD TEMPORAL → EJECUTAR → CERRAR → TERMINAR

La biometría demuestra presencia. No debería convertirse automáticamente en autoridad permanente.

Verificar el dato biométrico. No almacenar indefinidamente el encuentro.

La biometría adquiere cada vez mayor importancia para la identidad digital. Las huellas dactilares, los rasgos faciales, los patrones del iris, la voz y otras características biológicas pueden aportar pruebas sólidas de la presencia de una persona determinada.

Pero la biometría presenta un problema de ciberseguridad singular: una contraseña puede cambiarse; un rostro o una huella humana no pueden sustituirse fácilmente.

AttesTorr separa, por tanto, la prueba biométrica de la autoridad persistente de la máquina.

La aplicación o el servidor protegido no necesitan recibir ni almacenar el dato biométrico bruto. En su lugar, pueden recibir el resultado necesario para la operación autorizada.

Los datos biométricos que legítimamente deban persistir requieren protección apropiada. AttesTorr no implica que toda referencia biométrica pueda o deba desaparecer. La distinción se da entre la infraestructura de identidad necesaria y la persistencia innecesaria de cada interacción biométrica.

El registro inicial, el almacenamiento de plantillas, la integridad del dispositivo de captura, la precisión de la comparación y las copias conservadas por proveedores de identidad siguen siendo responsabilidad de esos sistemas, salvo que se incluyan explícitamente y se acrediten mediante pruebas dentro del límite de confianza declarado.

8. CONTENCIÓN DE LA IA

La IA amplía la ciberseguridad más allá de las cuentas humanas. Un sistema de IA puede actuar, recuperar información, inferir, invocar herramientas, generar código, acceder a bases de datos, comunicarse con servicios y operar a velocidad de máquina.

Esto plantea una nueva pregunta: ¿cuánta autoridad permanente debería poseer una IA?

Layer ZERO ofrece una respuesta arquitectónica: convocar la inteligencia para la tarea en vez de concederle autoridad perpetua.

Una ejecución de IA puede admitirse con un propósito definido, limitarse a recursos autorizados, recibir identidad temporal, impedirle persistencia irrestricta, restringir sus exportaciones, cerrarse al concluir y exigir que vuelva a reunir los requisitos para la siguiente ejecución.

Esto distingue entre capacidad de IA y autoridad de IA. Una inteligencia poderosa no necesita acceso permanente.

Layer ZERO limita si se admite una ejecución de IA, cuánto dura su autoridad y qué evidencia debe dejar. No demuestra que las salidas de un modelo sean correctas, seguras, justas, imparciales o apropiadas para usos de gran trascendencia. La evaluación de modelos, la gobernanza de políticas y la seguridad de las aplicaciones siguen siendo necesarias.

9. APLICACIÓN DE CONTROLES EN LA PUERTA DE ENLACE

PERSONA / IA / DISPOSITIVO → ADMISIÓN Y VINCULACIÓN → EJECUCIÓN GOBERNADA → CIERRE → EVIDENCIA DE CIERRE → EXPORTACIÓN AUTORIZADA

Layer ZERO define las restricciones rectoras; cada bloque constituye una responsabilidad asignada de aplicación o evidencia. La exportación, cuando se autoriza, ocurre solo después del cierre. La verificación independiente es una evaluación separada de solo lectura, posterior al cierre.

Cuando una implementación sitúa una puerta de enlace frente a la infraestructura protegida, cambia el modelo tradicional de conexión. Esa puerta aplica las restricciones de Layer ZERO; no es por sí misma una autoridad de admisión. Layer ZERO es la arquitectura rectora, no una puerta de enlace, proxy o servicio situado en la ruta de red; la admisión sigue correspondiendo a la función designada por la arquitectura.

En este modelo, poseer una credencial convencional no implica necesariamente autoridad irrestricta sobre el servidor. El sistema puede determinar quién o qué solicita una ejecución, por qué, qué recursos puede tocar, qué información puede entrar, persistir o salir, cuánto dura la autoridad y si el cierre se completó correctamente.

Por tanto, la puerta de enlace pasa a ser un punto de aplicación de la autoridad de ejecución, no simplemente un filtro de tráfico. No se convierte en nueva fuente de admisión o finalidad, ni considera suficientes para la admisión una credencial convencional, ubicación de red, conexión exitosa o estado operativo.

10. DENEGACIÓN POR DEFECTO ANTE FALLOS

Una arquitectura de seguridad efímera no puede depender exclusivamente de afirmaciones de que se produjo una eliminación. El cierre debe poder aplicarse y verificarse.

Por ello, la arquitectura de AttesTorr favorece el comportamiento de denegación ante fallos: si no puede establecerse la autorización exigida, no admitir; si no pueden mantenerse las condiciones de ejecución, no continuar; si no se satisfacen las condiciones de exportación, no exportar; y si la evidencia de cierre está incompleta o no puede verificarse, el verificador no reconoce la finalidad.

Para un cierre que sustenta afirmaciones de aseguramiento, la supervisión, los registros, los mensajes de apagado y las declaraciones de operadores no sustituyen la evidencia de cierre completa, actual y correctamente firmada. La finalidad solo se alcanza mediante la evaluación que haga un verificador independiente de esa evidencia; la evidencia incompleta o contradictoria implica rechazar la afirmación.

Esto convierte la evidencia de una función de observación en parte de la arquitectura de seguridad.

11. EVIDENCIA SIN RETENER EL EVENTO

Una distinción fundamental de AttesTorr es que la evidencia puede sobrevivir sin que tenga que sobrevivir la ejecución subyacente.

Una organización puede necesitar pruebas de que una identidad autorizada estuvo presente, de que se cumplieron condiciones requeridas, ocurrió una transacción, se permitió una salida específica, se inició el cierre o se satisficieron condiciones de desmantelamiento esperadas.

Eso no exige necesariamente conservar todos los datos sensibles de entrada, estados intermedios, muestras biométricas, interacciones con IA o entornos de sesión.

El resultado deseado es evidencia sin persistencia innecesaria. Esto puede reducir la tensión entre ciberseguridad, privacidad, responsabilidad y auditoría.

Evidencia sin persistencia innecesaria.

12. SEGURIDAD EN LA ERA CUÁNTICA

Proteger lo que debe persistir. Minimizar lo que debe persistir.

A menudo se describe la computación cuántica como si fuera a volver obsoleta toda la criptografía. Eso es incorrecto.

Las computadoras cuánticas a gran escala suponen una amenaza seria para varios sistemas criptográficos de clave pública ampliamente implantados, razón por la cual ya se están desplegando estándares criptográficos poscuánticos.

AttesTorr no sustituye a la criptografía: la complementa. La criptografía poscuántica aborda cómo proteger información y relaciones criptográficas que deban sobrevivir. La arquitectura efímera aborda otra pregunta: ¿qué información y autoridad necesitan sobrevivir en primer lugar?

Todo lo que legítimamente sobreviva —incluidas credenciales de larga duración, firmas, exportaciones permitidas, recibos u otras pruebas— debe emplear protección criptográfica adecuada, incluidos mecanismos resistentes a la computación cuántica cuando se requieran.

La contribución de AttesTorr no es afirmar una ejecución a prueba de ataques cuánticos. Su aporte arquitectónico es distinto: un futuro avance criptoanalítico no puede descifrar información sensible que nunca se retuvo innecesariamente para ser atacada. Eso no protege textos cifrados ya interceptados, copias previas o externas, exportaciones autorizadas ni las claves, firmas y pruebas que deban persistir;

todo ello sigue necesitando protección criptográfica, incluidos mecanismos poscuánticos cuando corresponda.

13. LA CIBERSEGURIDAD COMO FUNCIÓN DEL TIEMPO

La ciberseguridad tradicional suele tratar los datos principalmente como activos. AttesTorr añade otra dimensión: la duración.

La exposición de seguridad asociada con información o autoridad depende no solo de su valor, sino también de cuánto tiempo permanece disponible. Conceptualmente, la exposición se relaciona con el estado atacable multiplicado por el tiempo.

Esta es una regla orientativa explicativa, no una fórmula de riesgo validada. El riesgo también depende de la accesibilidad, privilegios, vulnerabilidades, controles, capacidad del adversario y consecuencias. Toda afirmación cuantificada de eficacia requiere un método de medición, entorno y pruebas definidos.

Reducir cualquiera de los dos factores puede reducir la oportunidad. Reducir ambos cambia la arquitectura.

La persistencia no es neutral. La persistencia crea tiempo de exposición. Por ello, el control del ciclo de vida se convierte en un elemento fundamental de la ciberseguridad.

14. LO QUE ATTESTORR NO AFIRMA

AttesTorr no afirma que los sistemas efímeros no puedan contener vulnerabilidades; que los atacantes no puedan actuar durante una ejecución activa; que toda la información deba desaparecer; que todo mecanismo de persistencia sea perjudicial; que la criptografía sea innecesaria; que la biometría sea intrínsecamente segura; que la computación cuántica deje de importar; que el hardware sea perfectamente fiable; que siempre pueda demostrarse la ausencia física de cada byte en toda ubicación posible; ni que una arquitectura pueda declararse imposible de vulnerar.

La propuesta es más acotada y defendible: un sistema puede reducir la exposición cibernética limitando deliberadamente la existencia, duración, autoridad, recuperabilidad y continuidad del estado sensible de ejecución.

Estas propiedades deben demostrarse finalmente mediante implementación, pruebas, verificación independiente y límites de confianza claramente declarados.

En particular, reducir superficie y ventana de ataque son objetivos de diseño, no garantías de ausencia de vulnerabilidades, copias fuera del límite u otra persistencia. La duración de la ejecución es una dimensión de exposición, no una medida autónoma de riesgo: no se afirma ninguna proporción universal de reducción ni inmunidad mientras la ejecución está activa.

Solo puede sobrevivir la evidencia cuya persistencia autoriza la arquitectura, y esa evidencia no debe transportar por sí misma estado sensible de ejecución. La existencia de un recibo no establece por sí sola la validez de una afirmación; siguen aplicándose integridad, actualidad, autoridad de emisión y validación independiente. Las garantías sustentadas por evidencia quedan limitadas a un límite de confianza declarado, versionado y vinculado criptográficamente mediante hash. Los supuestos sobre proveedores, la persistencia fuera de ese límite y otros riesgos residuales se divulgan en lugar de tratarlos como ausentes de manera demostrada.

15. EL MODELO DE CIBERSEGURIDAD DE LAYER ZERO

El modelo de ciberseguridad de AttesTorr puede resumirse en seis principios.

1. MINIMIZAR LA EXISTENCIA — No conservar estado sensible solo porque la infraestructura facilite su persistencia.
2. MINIMIZAR LA AUTORIDAD — Conceder únicamente la autoridad necesaria para la ejecución.
3. MINIMIZAR LA DURACIÓN — Terminar el estado de ejecución y la autoridad temporal cuando termine su propósito.
4. MINIMIZAR LA EXPORTACIÓN — Solo la información autorizada cruza el límite de ejecución.
5. VERIFICAR EL CIERRE — No equiparar un mensaje de software que dice «eliminado» con una finalidad respaldable de forma independiente.
6. EXIGIR AUTORIDAD NUEVA — No permitir que una ejecución exitosa se convierta silenciosamente en autoridad permanente.

En conjunto: ADMIT → BIND → EXECUTE → CLOSE → SUCCESSOR

La verificación independiente de la evidencia de cierre sigue a un ciclo de vida completado. No es una fase de ejecución, ni una fuente de autoridad sucesora, ni un resultado portátil de finalidad.

CONCLUSIÓN

La industria de la ciberseguridad se ha vuelto extraordinariamente sofisticada al proteger lo que permanece. AttesTorr se pregunta si todo eso debería permanecer.

La pregunta cobra cada vez mayor importancia conforme los sistemas de IA adquieren autoridad de máquina, la biometría se vuelve infraestructura de identidad, los servidores acumulan cada vez más datos y la computación cuántica obliga a reconsiderar los supuestos criptográficos de larga duración.

La próxima frontera de la ciberseguridad quizá no sea simplemente un muro más fuerte alrededor de un patrimonio digital cada vez mayor. Tal vez sea un patrimonio más pequeño, de menor duración: un entorno en el que la autoridad sea temporal, la ejecución sensible esté delimitada, la persistencia exija justificación, el cierre forme parte de la arquitectura y el atacante se enfrente continuamente a un objetivo menguante.

Minimizar lo que puede ser atacado. Minimizar durante cuánto tiempo puede ser atacado. Minimizar lo que permanece después de que se cierra la ventana de ataque.

Menos persistencia. Menos exposición. Menos oportunidades.

La próxima frontera de la ciberseguridad es la propia existencia.

NOTA DE REFERENCIA

Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST), Proyecto de Criptografía Poscuántica. NIST ha estandarizado algoritmos criptográficos poscuánticos y recomienda planificar la migración de los sistemas que dependen de criptografía vulnerable a computadoras cuánticas suficientemente capaces.

<https://www.nist.gov/pqc>

MADUREZ Y LÍMITES DE LAS AFIRMACIONES

Este documento técnico describe una tesis arquitectónica y una dirección de producto. Las propiedades de seguridad dependen de la implementación, el perfil de despliegue, los supuestos sobre hardware y software, las decisiones de integración, los métodos de verificación y los límites de confianza declarados. Las afirmaciones deben respaldarse mediante implementaciones de referencia, pruebas, verificación independiente y evidencia operativa.