TEC360 Be Smart & Secure

okta The World's Identity Company™

White Paper:

Identidad como Infraestructura: Modelo Estratégico para Gobernar las Identidades Invisibles

TEC360 CLOUD
EN COLABORACIÓN CON
JUAN IGNACIO TORRES

Índice

4. Tipos de Identidad y Cómo se Proyectan

4.1 Identidad humana
4.2 Identidad de dispositivo
4.3 Identidad de sensor
4.4 Identidad de actuador
4.5 Workload Identity
4.6 Runtime Identity
4.7 Identidad de Mesh y Control-plane
4.8 Cómo Workload + Runtime Identity elimina riesgos modernos
4.9 OAuth, SPIFFE y WIMSE como bases tecnológicas
4.10 Activos y supply chain como extensiones del modelo

5. Validación de Identidades No Humanas (NHI)

5.1 La validación como base de Zero Trust
5.2 Marco universal de 9 pasos
5.3 Validación según cada tipo de identidad
5.4 Fuentes autoritativas múltiples
5.5 Ciclo de vida NHI

6. Plano de Autorización + Zero Trust Moderno

6.1 Identidad vs Autorización (diferencia crucial)
6.2 Verificación continua basada en evidencia
6.3 Delegación: reglas, riesgos, límites
6.4 Modelos PBAC, ABAC y ReBAC
6.5 Grupos: útiles pero insuficientes
6.6 Dominios y tenancy
6.7 Privilegios altos bajo JIT + attestation
6.8 Autorización para APIs y agentes IA
6.9 Autorización basada en runtime identity
6.10 El flujo completo Zero Trust (PIP–PDP–PEP + CAEP)
6.11 Implementaciones reales: Entra, Okta, SPIFFE, WIMSE, CAEP

7. Proceso de Implementación de NHI Governance (NHI-GA)

7.1 Por qué no repetir el modelo IGA tradicional
7.2 Punto de inicio: riesgo + objetivo empresarial
7.3 Selección del dominio crítico (APIs, pipelines, IA, OT, workloads)
7.4 Diseño del modelo de identidad
7.5 Integración del plano Zero Trust

CAPÍTULO 1 — CONTEXTO ESTRATÉGICO

Vivimos en un entorno digital donde las organizaciones dependen de servicios distribuidos, arquitecturas en nubes múltiples, flujos automatizados, APIs que conectan negocios completos, pipelines que despliegan software a escala y agentes de IA que procesan información en tiempo real.

En este nuevo contexto, las identidades ya no son únicamente personas. La operación moderna está sostenida por identidades no humanas (NHI): servicios, workloads, APIs, contenedores, modelos de IA, dispositivos, tokens, certificados, microservicios, sensores y actuadores.

La transformación es tan profunda que muchas empresas ya administran:

- **Más identidades no humanas que humanas**, en proporciones de 10:1 hasta 40:1.
- Automatizaciones que dependen de **tokens y secretos** que no tienen dueño claro.
- Ambientes cloud donde cada despliegue genera decenas de identidades efímeras.
- Agentes de IA que operan sin trazabilidad de identidad ni auditoría**.**

1.1 LA EXPLOSIÓN DE IDENTIDADES NO HUMANAS

La digitalización acelerada, la IA generativa, la automatización y el paso a arquitecturas distribuidas crearon un entorno donde:

- Cada microservicio tiene su propia identidad.
- Cada API requiere tokens, certificados y políticas de acceso.
- Cada pipeline CI/CD genera credenciales temporales.
- Cada modelo de IA actúa como entidad autónoma.
- Cada workload requiere identidad runtime para conectarse a otros servicios.

Lo que antes se consideraba “infraestructura técnica” hoy se ha convertido en “infraestructura de identidades”.

CAPÍTULO 1 — CONTEXTO ESTRATÉGICO

Vivimos en un entorno digital donde las organizaciones dependen de servicios distribuidos, arquitecturas en nubes múltiples, flujos automatizados, APIs que conectan negocios completos, pipelines que despliegan software a escala y agentes de IA que procesan información en tiempo real.

En este nuevo contexto, las identidades ya no son únicamente personas. La operación moderna está sostenida por identidades no humanas (NHI): servicios, workloads, APIs, contenedores, modelos de IA, dispositivos, tokens, certificados, microservicios, sensores y actuadores.

La transformación es tan profunda que muchas empresas ya administran:

- **Más identidades no humanas que humanas**, en proporciones de 10:1 hasta 40:1.
- Automatizaciones que dependen de **tokens y secretos** que no tienen dueño claro.
- Ambientes cloud donde cada despliegue genera decenas de identidades efímeras.
- Agentes de IA que operan sin trazabilidad de identidad ni auditoría**.**

1.1 LA EXPLOSIÓN DE IDENTIDADES NO HUMANAS

La digitalización acelerada, la IA generativa, la automatización y el paso a arquitecturas distribuidas crearon un entorno donde:

- Cada microservicio tiene su propia identidad.
- Cada API requiere tokens, certificados y políticas de acceso.
- Cada pipeline CI/CD genera credenciales temporales.
- Cada modelo de IA actúa como entidad autónoma.
- Cada workload requiere identidad runtime para conectarse a otros servicios.

Lo que antes se consideraba “infraestructura técnica” hoy se ha convertido en “infraestructura de identidades”.

1.2 RIESGOS CRECIENTES Y DOCUMENTADOS

Los incidentes recientes muestran que:

- Las identidades de máquina son actualmente el vector más explotado.
- La mayoría de breaches no ocurren por hackers sofisticados, sino por credenciales técnicas expuestas o tokens con excesivos permisos.
- Servicios críticos dependen de certificados que expiran sin monitoreo.
- Integraciones SaaS mantienen permisos ilimitados durante años.
- Workloads se comunican con otros servicios sin verificación criptográfica.

Los atacantes entendieron algo antes que la industria:

"El camino más fácil no es comprometer a un usuario humano, sino una identidad técnica."

1.3 LA BRECHA ENTRE IAM TRADICIONAL Y LA REALIDAD MODERNA

IAM nació para gobernar:

- Empleados
- Contratistas
- Proveedores

Accesos a aplicaciones "monolíticas"

Pero la realidad actual incluye:

- Workloads efímeros
- APIs públicas y privadas
- Automatizaciones CI/CD
- Integraciones SaaS
- Identidad de dispositivos
- Service Mesh
- Agentes autónomos de IA

IAM nunca fue diseñado para este volumen ni para esta dinámica.

11.4 IMPACTO DIRECTO EN INDUSTRIAS

Fintech & Banca

- Tokens OAuth con privilegios excesivos manejan pagos y movimientos sensibles.
- Modelos de fraude y riesgo operan sin identidad verificable.

Retail & eCommerce

- Workloads que procesan inventario y logística carecen de validación continua.

Manufactura & OT

- Identity sprawl en sensores, actuadores y PLCs sin gobierno unificado.

Farmacéuticas & Supply Chain

- Servicios que manejan datos regulados sin trazabilidad de identidad.

1.5 POR QUÉ LAS NHI SON EL NUEVO PERÍMETRO EMPRESARIAL

La empresa moderna ya no se protege en redes, firewalls o segmentos.

- El perímetro hoy está en:
- Identidades humanas
- Identidades técnicas
- Identidades efímeras
- Identidades de IA
- Identidades de integraciones

El problema no es técnico.

Es conceptual.

Sin un **modelo unificado de identidad**, Zero Trust es imposible.

CAPÍTULO 2: FUNDAMENTOS DEL MODELO DE IDENTIDAD COMO INFRAESTRUCTURA

El modelo **Identidad como Infraestructura** parte de una premisa simple pero trascendental: **toda acción en un sistema digital es ejecutada por una entidad**, y toda entidad que ejecuta acciones debe tener una i**dentidad verificable** asociada a un conjunto de **atributos confiables.**

Este modelo corrige una limitación histórica del IAM tradicional: la dependencia casi exclusiva de la identidad humana como eje de gobernanza. En un mundo donde la operación digital está impulsada por APIs, workloads, agentes de IA, pipelines y microservicios, la identidad debe ser redefinida como un concepto **universal**, no humano y humano por igual.

2.1 ENTIDAD: EL ORIGEN DE TODO LO QUE ACTÚA EN EL SISTEMA

Una **entidad** es cualquier componente que puede ejecutar una acción dentro del entorno tecnológico:

- Un usuario
- Una API
- Un sensor
- Un servicio
- Un contenedor
- Un agente de IA
- Un dispositivo
- Un workload efímero
- Un pipeline
- Un servicio en mesh
- Un actuador

El criterio clave es: **Si actúa, es entidad.**

Entender este concepto unificado permite eliminar la fragmentación entre equipos donde cada uno utiliza vocabulario distinto para referirse a piezas del sistema.

La entidad existe **antes** de la identidad.

La identidad es una representación asignada; la entidad es el origen

2.2 IDENTIDAD: LA REPRESENTACIÓN VERIFICABLE DE UNA ENTIDAD

Una **identidad** es la forma en la que una entidad se presenta ante un sistema para

- Declarar quién es
- Ser verificada
- Obtener permisos
- Ejecutar acciones
- Ser auditada

La identidad no es el usuario ni el servicio: **es la representación digital creada para interactuar con otros sistemas.**

En el caso humano, suele ser una cuenta.

En máquinas, puede ser:

- Un certificado
- Un token
- Un SVID (SPIFFE)
- Un JWT con claims
- Una identidad runtime emitida por un mesh

Toda identidad debe ser:

- Única
- Verificable
- Trazable
- Asociada a atributos confiables
- Capaz de ser validada continuamente

2.3 ATRIBUTOS: EL CONJUNTO DE SEÑALES QUE PERMITEN VALIDAR UNA IDENTIDAD

Los atributos son la **evidencia estructural** que permite validar una identidad.

Son señales que describen **propiedades verificables** sobre una entidad o sobre su estado actual.

Tipos de atributos:

1. **Atributos identificadores**
   - Nombre
   - ID único
   - UID/GID
   - Service account name
   - SPIFFE ID
2. **Atributos criptográficos**
   - Llaves
   - Firmas
   - Hashes de integridad
   - Certificados
   - Token bindings
3. **Atributos operativos**
   - Tiempo de vida
   - Origen del despliegue
   - Versiones
   - Hash de imagen
   - Nodo, pod o cluster donde corre
4. **Atributos relacionales**
   - Qué servicios puede invocar
   - Qué datos puede consumir
   - Qué usuario o equipo es dueño
5. **Atributos de contexto**
   - Riesgo
   - Ubicación
   - Variación de comportamiento
   - Señales de seguridad (device posture, anomalías)

Los atributos son críticos porque permiten pasar de un modelo estático a uno **dinámico**, donde la autorización depende de condiciones vivas del sistema, habilitando Zero Trust real.

2.4 LA RELACIÓN ESTRUCTURAL: ENTIDAD → IDENTIDAD → ATRIBUTOS

El corazón del modelo es la relación: **Entidad → Identidad → Atributos**

- **Entidad:** el origen que actúa
- **Identidad:** su representación verificable
- **Atributos:** la evidencia que permite validar y autorizar

Si cualquiera de las tres piezas falla:

- Sin entidad definida, no existe contexto.
- Sin identidad, no se puede auditar ni autorizar.
- Sin atributos confiables, no se puede verificar.

Esta estructura habilita un lenguaje común entre:

- DevOps
- Seguridad
- Arquitectura
- Compliance
- Ingeniería de plataformas
- Equipos de datos
- Equipos de IA

Todos operan sobre el mismo marco conceptual.

2.5 QUÉ NO ES IDENTIDAD Y POR QUÉ ES CRÍTICO DIFERENCIARLO

Uno de los mayores problemas en organizaciones modernas es que aspectos técnicos **incorrectamente considerados como "identidades"** generan confusión, fallas de auditoría y riesgo.

→ • **Un asset NO es identidad**. Un repositorio, un bucket, una base de datos o una plantilla no actúan. Por lo tanto, no pueden tener identidad. Tienen dueño y custodio, pero no identidad.

→ • **Un rol NO es identidad**. Un rol describe permisos, no quién los ejerce.

→ • **Un certificado expirado no válida identidad**

Valida que **alguna vez** existió, pero ya no es confiable.

Diferenciar lo que sí y lo que no es identidad evita:

- Accesos fantasma
- Tokens huérfanos
- Roles sin dueño
- Workloads imposibles de rastrear
- Auditorías fallidas

2.6 IMPORTANCIA EJECUTIVA PARA CIOS, CISOS Y CTOS (GOBIERNO, RIESGO, TRAZABILIDAD)

Para los líderes tecnológicos, este modelo representa una transformación clave en cómo se gobierna la organización:

Gobierno: Permite tener un marco organizacional unificado para todos los equipos, eliminando vocabularios fragmentados y modelos incompatibles entre sí.

Riesgo: El riesgo de identidades invisibles es hoy uno de los mayores factores de brecha. El modelo permite visibilidad, validación continua y control centralizado.

Trazabilidad

Cada acción puede vincularse a una entidad clara, una identidad verificable, atributos validados, autorización basada en evidencia.
Esto transforma la forma en que se construyen auditorías, cumplimiento normativo, Zero Trust, modelos de automatización, marcos de diseño arquitectónico.
Es, en esencia, la base para operar una empresa digital moderna.

2.6 IMPORTANCIA EJECUTIVA PARA CIOS, CISOS Y CTOS (GOBIERNO, RIESGO, TRAZABILIDAD)

Para los líderes tecnológicos, este modelo representa una transformación clave en cómo se gobierna la organización:

Gobierno: Permite tener un marco organizacional unificado para todos los equipos, eliminando vocabularios fragmentados y modelos incompatibles entre sí.

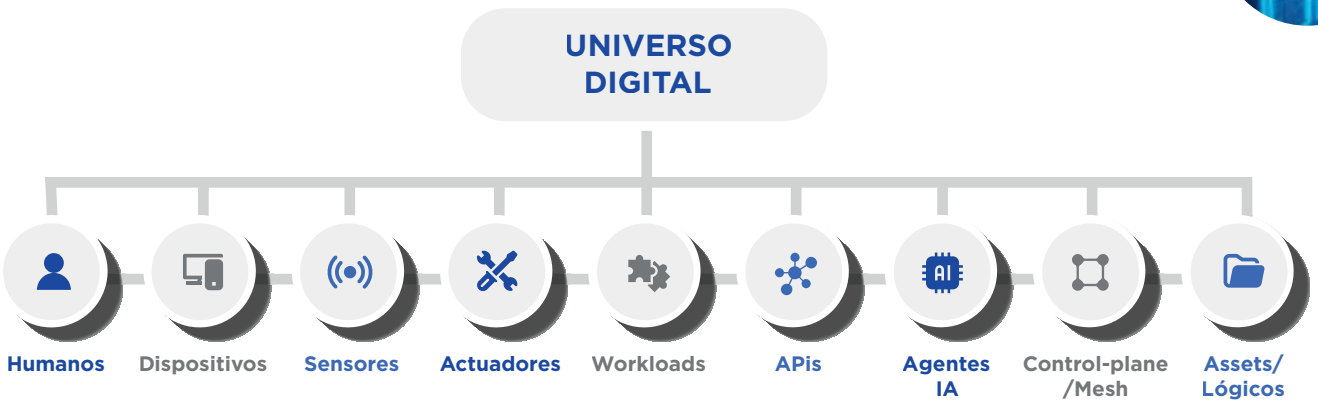
Riesgo: El riesgo de identidades invisibles es hoy uno de los mayores factores de brecha. El modelo permite visibilidad, validación continua y control centralizado.

Trazabilidad

Cada acción puede vincularse a una entidad clara, una identidad verificable, atributos validados, autorización basada en evidencia.
Esto transforma la forma en que se construyen auditorías, cumplimiento normativo, Zero Trust, modelos de automatización, marcos de diseño arquitectónico.
Es, en esencia, la base para operar una empresa digital moderna.

CAPÍTULO 3: EL MAPA DEL UNIVERSO DIGITAL MODERNO

La infraestructura digital moderna está compuesta por múltiples tipos de entidades que interactúan constantemente entre sí. Cada una de ellas juega un rol específico dentro de los flujos operativos del negocio. Comprender claramente este mapa es el primer paso para gobernar su identidad, su validación y su autorización dentro de un modelo Zero Trust.



UNIVERSO DE IDENTIDADES DIGITALES

La complejidad de este universo no proviene del volumen, sino de la **diversidad de entidades** que actúan simultáneamente: humanas, técnicas, efímeras, autónomas, distribuidas y con distintos niveles de privilegio.
Este capítulo establece una taxonomía clara para clasificar **qué existe, qué actúa** y qué **debe ser gobernado** bajo el modelo de Identidad como Infraestructura.

3.1 IDENTIDADES HUMANAS

Las identidades humanas son la base histórica de los sistemas IAM. Representan; empleados, proveedores, contratistas, terceros, clientes, colaboradores temporales.

Su ciclo de vida ha sido tradicionalmente estable (joiner → mover leaver). Sin embargo, su relevancia dentro del universo digital ha cambiado:

Son importantes porque:

- Son el origen de la delegación y responsabilidad.
- Determinan quién es accountable de identidades no humanas.
- Interactúan con sistemas que luego operan de manera autónoma

Son limitadas porque:

- Representan un porcentaje reducido del total de entidades.
- No sostienen la operación digital por sí mismas.
- No pueden abarcar la velocidad y escala de la automatización moderna.

En un mundo dominado por workloads, APIs y agentes de IA, la identidad humana ya no es el centro del sistema, pero sí sigue siendo el punto de responsabilidad organizacional.

3.2 DISPOSITIVOS

Los dispositivos son entidades físicas que actúan como puntos de ejecución para usuarios o servicios. Su identidad es fundamental porque:

Actúan como intermediarios entre:

- Usuarios y aplicaciones
- Servicios locales y servicios en la nube
- Agentes de seguridad y arquitecturas Zero Trust

Sus atributos aportan señales críticas:

- Integridad del dispositivo
- Estado de seguridad (parches, configuraciones, posture)
- Ubicación y variación de comportamiento
- Certificados o llaves utilizados para autenticación

Por qué son relevantes:

- Pueden ser comprometidos con gran facilidad.
- Pueden transportar credenciales técnicas.
- Son parte esencial del contexto en decisiones de autorización.

En Zero Trust, el dispositivo se evalúa tan estrictamente como al usuario:
no es suficiente saber quién es el usuario; también es necesario saber desde qué dispositivo actúa.

3.3 SENSORES, ACTUADORES Y ESTRUCTURAS LÓGICAS

Sensores: Los sensores representan entidades que generan datos del entorno físico y los proyectan hacia sistemas digitales. Aunque no siempre requieren una identidad compleja, su rol dentro de arquitecturas OT, IoT y espacios industriales es crítico: pueden influir en decisiones automatizadas y disparar procesos operativos. Lo esencial es validar su legitimidad, su origen y su integridad para evitar manipulación de datos, falsificación de señales o inyección de comportamientos maliciosos en flujos críticos de negocio.

Actuadores: Los actuadores no solo reportan información: ejecutan acciones. Son entidades que materializan decisiones técnicas en el mundo físico o industrial, abrir una válvula, detener un motor, modificar una línea de producción, activar un protocolo de seguridad. Por ello, requieren una gobernanza más estricta que los sensores. Toda acción debe estar respaldada por una identidad verificable, una política clara y evidencia contextual que confirme que la operación es legítima, autorizada y segura.

Estructuras Lógicas: Las estructuras lógicas, tales como colas de mensajes, tópicos, brokers, pipes o espacios de datos, no actúan por sí mismas, pero constituyen los canales a través de los cuales actúan otras identidades. Gobernarlas implica entender quién puede producir, consumir, orquestar o modificar flujos de información. Aunque no siempre requieren proyecciones de identidad explícita, sí necesitan controles de autorización, límites de acceso, validación de integridad y trazabilidad para evitar manipulación de datos o intercepciones invisibles dentro del ecosistema.

3. 4 WORKLOADS & SERVICIOS

Los workloads y servicios representan el núcleo operativo del negocio digital. Son las entidades que realmente “mueven” los sistemas:

- Servicios de pagos
- Microservicios de riesgo
- Pipelines de CI/CD
- Jobs de machine learning
- Workers de analítica
- Servicios que procesan transacciones
- Backends empresariales
- Sistemas automatizados que procesan tareas críticas

Sus características los hacen únicos:

- Existen en cantidades masivas.
- Son efímeros: nacen, mueren, escalan y mutan.
- Operan sin intervención humana.
- Interactúan con datos sensibles.
- Se comunican con múltiples sistemas simultáneamente.

Todo workload tiene **dos identidades:**
1. Workload Identity: Es la identidad declarada del servicio, que describe; su propósito, su dueño, su binario autorizado y su rol dentro de la arquitectura.
2. Runtime Identity: Es la identidad real de la instancia que se está ejecutando, validada por; certificados efímeros, hash del binario en ejecución, attestation criptográfica y atributos del cluster o nodo.

Por qué esto importa:
La seguridad moderna depende de validar que:
La instancia que está ejecutando código sea exactamente la instancia que debería existir.

3.5 AGENTES DE IA

La Inteligencia Artificial ha introducido una nueva clase de entidades: los agentes capaces de actuar autónomamente dentro de sistemas.

Estos agentes pueden:

- Invocar APIs
- Procesar información sensible
- Tomar decisiones
- Desencadenar acciones dentro de workflows
- Interactuar con identidades humanas y técnicas

Riesgos asociados:

- Operaciones autónomas sin trazabilidad.
- Acceso excesivo a datos sensibles.
- Uso de credenciales incrustadas.
- Ambigüedad sobre "quién" ejecutó una acción: ¿el usuario?, ¿el agente?, ¿otro servicio?

Requerimientos del modelo:

- Identidad única por agente o instancia del modelo.
- Trazabilidad completa de decisiones.
- Atributos que definan su capacidad operativa.
- Validación continua del entorno donde corre.
- Delegación humana explícita y auditable.

Los agentes de IA convierten la identidad en un elemento imprescindible para controlar autonomía, riesgo y comportamiento dentro del negocio.

3.6 SISTEMAS QUE GOBIERNAN A OTROS SISTEMAS (CONTROL-PLANE / MESH)

Los sistemas de control-plane y service mesh ocupan un lugar especial:
no solo actúan, sino que gobiernan cómo actúan otras entidades.

Incluyen:

- Kubernetes control plane
- Service meshes como Istio o Linkerd
- Orquestadores de contenedores
- Sistemas de colas y eventos
- Data mesh
- Motores de scheduling

Por qué requieren identidades más fuertes:

- Pueden crear o destruir recursos críticos.
- Emiten certificados y llaves.
- Definen el enrutamiento del tráfico.
- Asignan identidades runtime.
- Controlan políticas de seguridad.
- Intervienen en despliegues y mutaciones del sistema.

Si un control-plane es comprometido, **toda la infraestructura lo está**.
Por eso la identidad de estos sistemas requiere:

- Atributos criptográficos de alta seguridad
- Validación continua
- Aislamiento
- Autorización granular

3.7 ACTIVOS DIGITALES (SIN IDENTIDAD, PERO CON DUEÑO Y CUSTODIA)

Los activos digitales no son entidades, porque no actúan por sí mismos.
Aun así, representan elementos críticos que requieren gobierno.

Incluyen:

- Repositorios
- Buckets
- Artefactos de CI/CD
- Modelos de IA almacenados
- Plantillas
- Imágenes de contenedores
- Datos estructurados y no estructurados

Por qué no tienen identidad:

- No ejecutan acciones.
- No se autentican ante sistemas.

Por qué igual deben gobernarse:

- Pueden ser modificados maliciosamente.
- Influyen en la creación de identidades (ej. imágenes de contenedores).
- Son origen de supply chain attacks.
- Deben tener dueño humano responsable.

Los activos digitales son el **estado** de la infraestructura. Las identidades son los **actores. Ambos deben gobernarse en conjunto.**

CAPÍTULO 4: TIPOS DE IDENTIDAD Y CÓMO SE PROYECTAN

Cada tipo de entidad dentro del ecosistema digital requiere un modelo de identidad específico. Aunque todas comparten principios comunes —representación verificable, atributos confiables y validación continua— la forma en la que cada identidad se proyecta varía profundamente según su naturaleza, propósito y contexto operativo.

4.1 IDENTIDAD HUMANA

La identidad humana es la forma más antigua y conocida de identidad digital. Representa a empleados, contratistas, proveedores, clientes, socios y terceros autorizados.

Su proyección tradicional se basa en credenciales, atributos provenientes de HR, roles asignados, factores de autenticación y permisos definidos por pertenencia o función laboral.
En la era moderna, la identidad humana:

- Sigue siendo el origen de accountability.
- Representa la fuente de delegación hacia identidades no humanas.
- Se enriquece con señales de riesgo, dispositivo y comportamiento.

Sin embargo, ya no es el tipo de identidad dominante en términos de volumen ni en relevancia operativa.
Hoy, es el punto de responsabilidad, pero no el motor de la operación.

4.2 IDENTIDAD DE DISPOSITIVO

La identidad de dispositivo se proyecta para identificar el hardware que actúa en nombre de usuarios o servicios. Incluye; laptops, desktops, móviles, servidores, dispositivos especializados.
La identidad del dispositivo aporta atributos críticos:

- integridad del sistema,
- postura de seguridad,
- estado de parches,
- ubicación,
- certificación asociada.

Estos atributos influyen directamente en decisiones de autorización, especialmente dentro de modelos Zero Trust.
Un usuario autenticado desde un dispositivo comprometido o no verificado representa riesgo.

4.3 IDENTIDAD DE SENSOR

Los sensores recopilan señales y las transmiten a otros sistemas.
Cada sensor necesita identidad para validar su autenticidad, correlacionar su información, garantizar que los datos no fueron falsificados e integrar atributos físicos, lógicos o de entorno.
Su identidad incluye:

- número de serie,
- certificados embebidos,
- llaves de manufactura,
- atributos de entorno,
- firmware autorizado.

La identidad de sensor protege flujos críticos como manufactura, logística, salud, monitoreo industrial y ecosistemas OT.

4.4 IDENTIDAD DE ACTUADOR

A diferencia de los sensores, los actuadores modifican el entorno.
Su identidad debe ser aún más fuerte, porque sus acciones encienden o apagan maquinaria, abren compuertas, modifican flujos industriales y alteran variables de procesos críticos.

La identidad de actuador debe garantizar:

- que el dispositivo es legítimo,
- que el comando recibido es válido,
- que el firmware no fue alterado,
- que la acción está autorizada por la política correspondiente.

Sin identidad robusta, un actuador comprometido se convierte en un vector de riesgo físico y operativo.

4.5 WORKLOAD IDENTITY

Workload Identity representa la identidad declarada de un servicio. Incluye el nombre del servicio, su propósito, su equipo dueño, su imagen o binario autorizado, atributos operativos (versión, entorno, región), credenciales derivadas (certificados, llaves, tokens).

Workload Identity permite:

- aplicar políticas basadas en propósito,
- definir límites de acceso,
- crear trazabilidad del servicio,
- establecer controles previos al despliegue.

Sin Workload Identity definida, un servicio no puede participar en un modelo Zero Trust.

4.6 RUNTIME IDENTITY

Runtime Identity es la identidad de la instancia que realmente está ejecutándose.
Es efímera y depende del contexto en tiempo real.

Comparación Workload Identity vs Runtime Identity

Workload Identity

- Nombre del servicio
- Registro de aplicación
- Roles IAM asignados
- Entorno (dev/qa/prod)
- Versiones aprobadas
- Metadatos declarativos

Identidad estable declarada por la organización

coopera

valida

Runtime Identity

- Hash binario
- Certificado SVID/mTLS
- Integridad (TPM/enclave)
- Fuente del pipeline
- Contexto de ejecución
- Tiempo de vida (TTL)

Identidad de la instancia en ejecución

Incluye atributos como hash del binario ejecutado, certificados efímeros (mTLS/SVID), nodo, pod o contenedor donde corre, políticas aplicadas en runtime, grado de riesgo actual y señales de integridad y attestation.

Runtime Identity garantiza que:
La instancia que opera es legítima, íntegra y autorizada para actuar en ese momento.

Es el componente más crítico para seguridad moderna y Zero Trust continuo.

4.7 IDENTIDAD DE MESH Y CONTROL-PLANE

Los sistemas de mesh y control-plane gobiernan cómo interactúan otras entidades.

Su identidad permite autenticar componentes internos, emitir certificados, validar workloads, definir rutas de tráfico y aplicar políticas de seguridad distribuidas.

Dado su nivel de privilegio, la identidad de control-plane debe ser altamente verificable, aislada, auditada, con attestation fuerte, con políticas estrictas de rotación.

Estos sistemas no solo poseen identidad: **son emisores y validadores de identidad** para gran parte del entorno.

4.8 CÓMO WORKLOAD + RUNTIME IDENTITY ELIMINA RIESGOS MODERNOS

La combinación de:

- **Workload Identity (qué debe existir)**
- **Runtime Identity (qué está realmente ejecutándose)**

permite resolver los riesgos que históricamente han provocado brechas:

- imágenes manipuladas,
- servicios falsos,
- instancias no autorizadas,
- tokens comprometidos,
- tráficos entre servicios sin verificación,
- instancias corriendo versiones no aprobadas.

Juntas habilitan:

- integridad verificable,
- autorización basada en evidencia,
- validación continua,
- trazabilidad completa de acciones técnicas.

Este es el núcleo operativo del modelo de Identidad como Infraestructura.

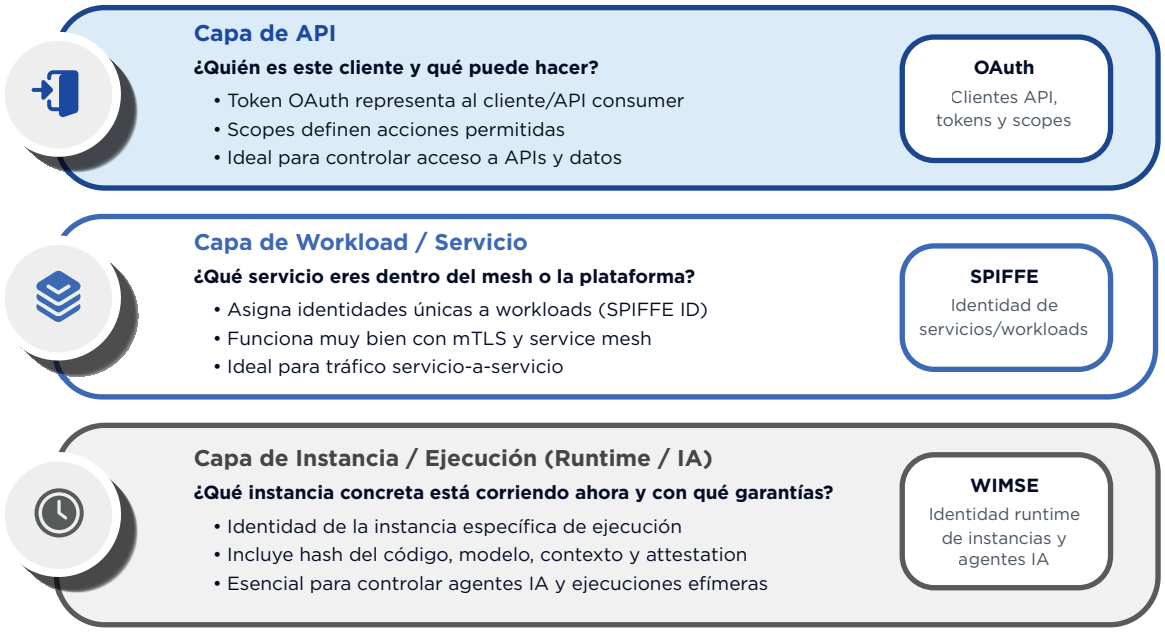
4.9 OAUTH, SPIFFE Y WIMSE COMO BASES TECNOLÓGICAS

OAuth: Proyecta identidad y autorización para APIs, aplicaciones, integraciones SaaS y clientes. Permite delegación controlada mediante scopes.

SPIFFE / SVID: Define estándares de identidad para workloads, emitiendo certificados verificables que representan servicios y procesos distribuidos.

WIMSE: Extiende identidad runtime a entornos sin service mesh, agentes de IA y workloads que no pueden integrarse a un mTLS tradicional.

Tres capas de identidad técnica: OAuth, SPIFFE y WIMSE



OAuth, SPIFFE y WIMSE no compiten: se complementan en capas distintas de identidad técnica.

Estas tecnologías materializan el modelo de identidad moderna y habilitan Zero Trust a nivel de servicio.

4.10 ACTIVOS Y SUPPLY CHAIN COMO EXTENSIONES DEL MODELO

Los activos digitales no actúan, pero influyen directamente en identidades como imágenes, artefactos, modelos de IA, plantillas, buckets y repositorios. Son el origen de workloads, pipelines, agentes de IA y certificados.

Por ello, deben gobernarse mediante un dueño humano, políticas de custodia, validación de integridad, controles de supply chain y auditoría continua.

Cuando un activo es comprometido, todas las identidades generadas a partir de él quedan en riesgo.

Estas entidades no tienen identidad porque no ejecutan acciones, pero son esenciales porque contienen la información y los componentes con los que trabajan todos los servicios.
Incluyen:

- repositorios de código,
- datasets,
- documentos,
- artefactos CI/CD,
- imágenes de contenedor,
- certificados y llaves,
- IaC,
- dominios, grupos, folders, namespaces.

Estas entidades son críticas porque:

A. Definen el comportamiento de las identidades activas

De aquí provienen:

- el código del servicio,
- la imagen,
- el hash autorizado,
- las políticas de configuración.

B. Son los objetos que las identidades consultan y manipulan
Ejemplos reales:

- payments-api escribe transacciones,
- fraud-engine consume modelos y patrones,
- pricing-agent analiza documentos de tarifas,
- inventory-ms actualiza tablas de stock,
- closing-etl mueve datos regulatorios.

C. Son la base del supply chain
Firmas, SBOM, SLSA, OCI trust, in-toto.

D. Conectan identidades con responsabilidad
Cada repositorio, dataset o imagen tiene dueño y custodio.

Esto permite trazar:
"Este servicio ejecutó esta acción sobre este activo bajo la responsabilidad de este equipo."
Son el punto donde el impacto del sistema se vuelve tangible.

CAPÍTULO 5: VALIDACIÓN DE IDENTIDADES NO HUMANAS (NHI)

La validación de identidad es el núcleo operativo de cualquier estrategia Zero Trust moderna. Tanto **NIST SP 800-207 (Zero Trust Architecture)** como el **CISA Zero Trust Maturity Model** establecen un principio fundamental:
Nada ni nadie se considera confiable por defecto. Toda identidad debe demostrar quién es, con evidencia verificable, antes de actuar.

Sin embargo, mientras este principio está bien establecido para identidades humanas (con marcos como NIST SP 800-63 o ISO/IEC 29003), **no existe un equivalente claro y completo para las identidades no humanas**, que hoy representan la mayoría de las transacciones, decisiones y acciones dentro de una organización moderna.

Además, otros estándares como:

- **ISO/IEC 29003 (Identity Proofing),**
- **SLSA / in-toto (integridad del software supply chain),**
- **NIST Risk Management Framework,**
- **NIST 800-53 (controles de seguridad)**

aportan piezas importantes, pero s**iguen dejando un vacío crítico: cómo validar sensores, actuadores, workloads, agentes de IA, instancias runtime, mallas de servicio, pipelines y repositorios.**

Este capítulo proporciona un enfoque práctico y gobernable para que el lector tenga clara la forma como se gobierna una identidad.

5.1 LA VALIDACIÓN COMO BASE DE ZERO TRUST

Zero Trust se fundamenta en la idea de que ninguna entidad debe recibir confianza por defecto. Esto incluye a las entidades no humanas, cuya actividad representa la mayor parte de la operación digital. La validación es, por tanto, el mecanismo que sostiene el principio de “verificar siempre”.

Validar una identidad implica confirmar:

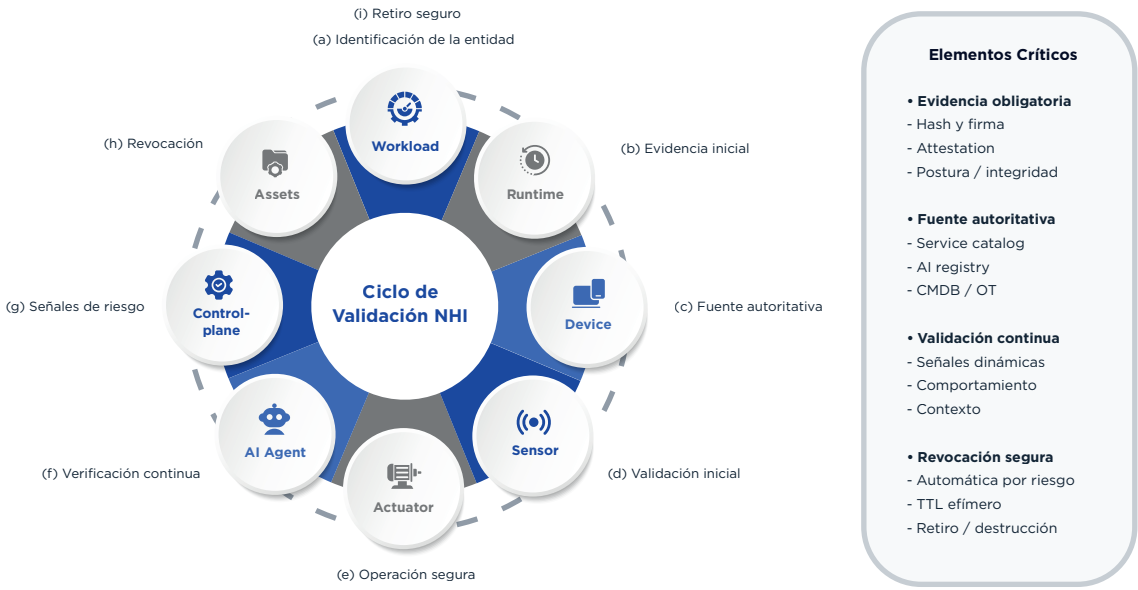
- **¿Qué entidad es?**
- **¿Cómo demuestra quién es?**
- **¿Con qué atributos cuenta?**
- **¿Si su estado actual es consistente con las políticas?**
- **¿Si mantiene integridad y legitimidad?**
- **¿Si existen riesgos contextuales que limiten su acción?**

La validación continua permite que Zero Trust opere más allá del punto de autenticación, integrándose en cada acción, cada interacción y cada decisión de autorización. Por eso, el NHI-GA debe estructurarse sobre tres pilares esenciales:

a. **Fuentes autoritativas diversas que convergen en un modelo único de gobierno.**
b. **Ciclos de vida específicos para cada subtipo de identidad.**
c. **Procesos de validación adecuados al riesgo, al contexto y a la naturaleza de la entidad.**

Estos pilares alinean la gobernanza con Zero Trust (NIST + CISA) y permiten que cada identidad opere bajo evidencia verificable.

Validación Continua de Identidades No Humanas (NHI)



Sin validación no puede existir autorización dinámica ni trazabilidad confiable.

.

La validación continua permite que Zero Trust opere más allá del punto de autenticación, integrándose en cada acción, cada interacción y cada decisión de autorización. Por eso, el NHI-GA debe estructurarse sobre tres pilares esenciales:

a. **Fuentes autoritativas diversas que convergen en un modelo único de gobierno.**
b. **Ciclos de vida específicos para cada subtipo de identidad.**
c. **Procesos de validación adecuados al riesgo, al contexto y a la naturaleza de la entidad.**

Estos pilares alinean la gobernanza con Zero Trust (NIST + CISA) y permiten que cada identidad opere bajo evidencia verificable.

5.2 MARCO UNIVERSAL DE 9 PASOS

La validación de identidades no humanas sigue un proceso estructurado que abarca todo el ciclo operativo. Este marco se inspira en ISO 29003, pero se amplía para cubrir las necesidades de entidades dinámicas, distribuidas y efímeras.

Los **nueve pasos** del proceso son:

1. **Identificación** | Determinar qué entidad requiere una identidad.
2. **Evidencia inicial** | Confirmar datos esenciales que prueban su existencia o legitimidad.
3. **Fuente autoritativa** | Validar la información contra un origen confiable.
4. **Validación previa** | Corroborar integridad, permisos y atributos antes de habilitar acciones.
5. **Operación segura** | Permitir la actividad solo bajo condiciones verificadas.
6. **Verificación continua** | Reevaluar atributos, riesgos e integridad en tiempo real.
7. **Monitoreo** | Registrar comportamientos, anomalías y desviaciones.

8. **Revocación** | Retirar acceso o identidad cuando ya no cumple políticas.
9. **Retiro** | Finalizar ciclo de vida y eliminar residuos digitales o credenciales.

Este marco proporciona un lenguaje común entre seguridad, arquitectura, DevOps, OT y equipos de IA

5.3 VALIDACIÓN SEGÚN CADA TIPO DE IDENTIDAD

La validación no es uniforme; depende del tipo de entidad y de su impacto en el sistema. Cada tipo requiere atributos distintos y métodos de verificación específicos.

Identidad humana: Se valida principalmente mediante biometría, MFA, atributos de HR, postura del dispositivo y patrones de comportamiento. Aunque no es el foco del marco NHI, sigue siendo la referencia primaria de accountability.

Identidad de dispositivo: Su validación depende de señales como integridad del sistema, postura de seguridad, certificación y conformidad con políticas corporativas. En Zero Trust, la identidad humana no se procesa sin validar el dispositivo simultáneamente.
Identidad de sensor: Debe validar autenticidad física, firmware autorizado, llaves de manufactura y origen del dato. Los sensores falsificados o manipulados son amenazas a procesos industriales, médicos o logísticos.

Identidad de actuador: Requiere validación más estricta, dado que produce efectos físicos. Debe confirmarse que el comando proviene de una entidad autorizada, con integridad de firmware y atributos correctos.

Workload Identity: La validación incluye integridad del binario, versión autorizada, equipo dueño, atributos declarados y permisos aprobados. Define qué servicio debe existir.

Runtime Identity: Su validación confirma qué instancia está realmente en ejecución, verificando certificados efímeros, hashes reales, contexto de cluster y señales de riesgo actuales. Define qué servicio está actuando en ese momento.

Identidad de Mesh y Control-plane: La validación exige la integridad completa del sistema que gobierna al resto, incluyendo su plane configurado, certificados raíz y atributos operativos. Un error aquí compromete toda la infraestructura.

Cada tipo de identidad requiere un método de validación adaptado a su comportamiento, riesgo y propósito.

5.4 FUENTES AUTORITATIVAS MÚLTIPLES

Ninguna identidad es válida sin una fuente autoritativa que confirme sus atributos. En identidades humanas, esta fuente suele ser HR; en identidades no humanas, el panorama es más diverso.
Las fuentes autoritativas pueden incluir

- Registros de manufactura (sensores, actuadores).
- Repositorios de artefactos (imágenes y binarios autorizados).
- Pipelines de CI/CD que certifican integridad
- Controles del service mesh.
- Información del control-plane.
- Firmas criptográficas o certificados raíz.
- Sistemas de inventario de workloads.

La validación depende de la confiabilidad de estas fuentes, y los sistemas deben diseñarse para extraer atributos desde el origen más preciso, no desde copias o configuraciones desactualizadas..

5.5 CICLO DE VIDA NHI

El ciclo de vida de una identidad no humana es más dinámico que el de una identidad humana.
Una identidad de servicio puede existir solo unos segundos, mientras que un sensor puede operar durante años.

El ciclo incluye:

- **Creación:** la identidad nace con atributos declarados o certificados.
- **Activación:** la entidad comienza a operar bajo políticas verificadas.
- **Uso continuo:** se ejecutan acciones bajo validación y autorización en tiempo real.
- **Actualización:** cambio de atributos, versión o binario.
- **Desactivación:** revocación cuando deja de ser necesaria.
- **Retiro:** eliminación completa y aseguramiento de que no persisten credenciales.

La clave en este ciclo es la validación continua:
en NHI no basta validar una vez; debe validarse cada vez que la entidad actúa.

CAPÍTULO 6: PLANO DE AUTORIZACIÓN + ZERO TRUST MODERNO

La autorización es el mecanismo que define qué acción puede realizar una identidad dentro de un sistema. En arquitecturas modernas, la autorización no puede depender únicamente de roles estáticos o permisos predefinidos; debe basarse en evidencia verificable que refleje la realidad de la entidad en cada momento.

Este capítulo describe el plano de autorización moderno: un componente dinámico, continuo y profundamente ligado al modelo de identidad y a la filosofía Zero Trust.

6.1 IDENTIDAD VS AUTORIZACIÓN (DIFERENCIA CRUCIAL)

La identidad define **quién es** una entidad; la autorización define **qué puede hacer.**

Modelo Zero Trust simplificado (NIST SP 800-207)

Confundir ambos conceptos es una de las principales causas de riesgo operativo.

Una identidad puede ser legítima y verificable, pero eso no significa que la acción solicitada deba ser permitida.

En Zero Trust, identidad y autorización son procesos distintos, cada uno con su propia evidencia, atributos y evaluación.

La identidad responde a autenticidad; la autorización responde a legitimidad de acción.

6.2 VERIFICACIÓN CONTINUA BASADA EN EVIDENCIA

La autorización moderna no se evalúa una única vez durante la autenticación. Debe evaluarse continuamente, porque los atributos que definen riesgo cambian en tiempo real.

La verificación continua analiza señales como; integridad del servicio, postura del dispositivo, reputación del usuario, política aplicada al workload, contexto geográfico o de red, variaciones de comportamiento, attestation del runtime y sensibilidad del recurso solicitado.

Flujo Zero Trust – Pipeline de Autorización (Estilo Híbrido)

Cada señal contribuye a determinar si la acción está alineada a las políticas de negocio. Zero Trust opera bajo esta regla: **toda acción requiere evidencia actualizada.**

6.3 DELEGACIÓN: REGLAS, RIESGOS, LÍMITES

Las identidades no humanas actúan en nombre de un humano o equipo. La delegación establece esa relación.

Una delegación sólida debe garantizar claridad de quién es dueño de qué identidad, límites bien definidos sobre lo que la identidad puede hacer, temporalidad sobre los privilegios otorgados, trazabilidad sobre cada decisión y acción así como la capacidad de revocar la delegación inmediatamente.

Delegación permitida vs no permitida

Delegación permitida

- ✓ Dentro de los límites definidos por identidad y política
- ✓ Basada en evidencia y contexto (rol, dominio, riesgo)
- ✓ Con vigencia temporal clara (TTL, expiración, revocación)
- ✓ Trazable y auditable (quién delega, a quién, para qué)

Ejemplos:

- Un owner delega la aprobación de accesos de su equipo
- Un responsable de servicio delega permisos temporales a un operador
- Un CISO delega la revisión inicial de riesgos a un equipo especializado
- Delegación vinculada a un dominio o alcance bien definido

Delegación no permitida

- ✗ Otorgar a otros permisos que el delegante no tiene
- ✗ Delegación sin evidencia ni justificación de negocio
- ✗ Delegación fuera del dominio o función de la identidad
- ✗ Delegaciones permanentes "para siempre" sin revisión
- ✗ Delegación circular (A delega en B y B en A) o cruzada entre áreas

Ejemplos:

- Un owner de servicio delega a un tercero ajeno a la organización
- Un operador delega privilegios de administración global
- Delegación usada para saltarse procesos de riesgo o cumplimiento
- Delegaciones que no quedan registradas ni son auditables

La delegación sin control genera identidades huérfanas, permisos excesivos y riesgos significativos al negocio.

6.4 MODELOS PBAC, ABAC Y REBAC

Los modelos modernos de autorización permiten describir políticas que consideran atributos, contexto, relaciones y riesgo.

PBAC (Policy-Based Access Control): Permite definir políticas expresivas que describen condiciones, reglas y evidencias requeridas para autorizar acciones.

ABAC (Attribute-Based Access Control): Las decisiones se basan en atributos del usuario, dispositivo, workload, recurso y contexto.

ReBAC (Relationship-Based Access Control): Evalúa relaciones entre entidades, como dependencias técnicas, jerarquías o dominios.

Los tres modelos pueden coexistir y se complementan dentro de estrategias Zero Trust.

6.5 GRUPOS: ÚTILES PERO INSUFICIENTES

Los grupos fueron creados para gestionar permisos humanos en aplicaciones tradicionales.
En entornos modernos tienen limitaciones:

- No incorporan atributos dinámicos.
- No reflejan integridad del workload.
- No capturan riesgo en tiempo real.
- No expresan relaciones entre servicios.

Aunque siguen siendo útiles para ciertos casos, no pueden ser el mecanismo principal en modelos distribuidos, automatizados y basados en evidencia.

6.6 DOMINIOS Y TENANCY

Las organizaciones modernas operan múltiples dominios; organizacionales, técnicos, tenants, ambientes aislados y entornos multi-cloud.

Cada dominio establece límites de confianza, políticas de interacción y visibilidad.
Una identidad válida en un dominio puede no ser válida en otro.
La autorización debe evaluar a qué dominio pertenece la identidad, qué recursos existen en ese dominio, qué políticas son aplicables y qué relaciones están permitidas.

El modelo multi-tenant exige atribución precisa y segura de cada identidad a su espacio operativo.

6.7 PRIVILEGIOS ALTOS BAJO JIT + ATTESTATION

Los privilegios elevados representan uno de los puntos más sensibles en cualquier arquitectura. Zero Trust exige minimizar su duración y alcance. El modelo moderno combina:

Just-In-Time (JIT): Privilegios que se activan solo cuando se necesitan y durante el menor tiempo posible.

Attestation: Validación criptográfica de que el servicio o workload mantiene integridad y ejecuta el binario autorizado.

Sin attestation, un privilegio JIT puede otorgarse a una entidad comprometida.
JIT y attestation deben operar juntos.

6.8 AUTORIZACIÓN PARA APIS Y AGENTES IA

APIs y agentes de IA requieren autorización mucho más granular y contextual que los usuarios o servicios tradicionales.

En APIs, la autorización depende de scopes, claims, contexto del cliente, riesgo del flujo y volumen o sensibilidad de la operación.

En agentes de IA, la autorización depende de la identidad del agente, acción que intenta ejecutar, trazabilidad del origen, requerimientos de delegación humana e impacto potencial en datos sensibles.

Sin autorización dinámica y clara, los agentes de IA pueden amplificar riesgos técnicos y operativos.

TEC360
Be Smart & Secure

White Paper:
Gobernanza Total para Humanos, Máquinas e IA

6.9 AUTORIZACIÓN BASADA EN RUNTIME IDENTITY

La autorización más fuerte no se basa en la identidad declarada del servicio, sino en su **runtime identity.**
Runtime identity permite confirmar:

- qué instancia está ejecutándose realmente,
- si el binario coincide con el autorizado,
- si el workload está en un entorno confiable,
- si mantiene integridad comprobada

La autorización basada en runtime identity reduce riesgos como workloads falsos, instancias inyectadas, servicios corriendo versiones manipuladas y accesos indebidos entre máquinas. Es el componente operativo esencial de Zero Trust moderno.

6.10 EL FLUJO COMPLETO ZERO TRUST (PIP–PDP–PEP + CAEP)

La autorización moderna se implementa mediante un flujo arquitectónico estándar:

- **PIP (Policy Information Point)** – recopila señales y atributos.
- **PDP (Policy Decision Point)** – evalúa políticas y toma decisiones.
- **PEP (Policy Enforcement Point)** – aplica la decisión.
- **CAEP (Continuous Access Evaluation Protocol)** – reevaluación continua basada en eventos y cambios de contexto.

Este flujo permite que la autorización sea dinámica, inmediata y ajustada a la realidad de cada acción.

6.11 IMPLEMENTACIONES REALES: ENTRA, OKTA, SPIFFE, WIMSE, CAEP

El modelo descrito no es teórico. Hoy existe soporte tecnológico amplio para implementarlo:

- **Microsoft Entra** habilita políticas dinámicas basadas en atributos y CAEP.
- **Okta** permite decisiones de acceso basadas en riesgo, señales y contexto.
- **SPIFFE/SVID** implementa identidad de workloads con certificados verificables.
- **WIMSE** opera identidad runtime en entornos sin service mesh o en agentes de IA.
- **CAEP** habilita autorización continua y adaptativa.

Modelos de Implementación Zero Trust – Comparación Ejecutiva

	Entra	Okta	WIMSE	CAEP
Runtime Identity	Workload IDs	Workflows	Identidades efímeras	Depende del PDP
PBAC	Conditional Access	Okta Policy	Policies workload	Core CAEP
Evaluación continua	Basado en señales	Por eventos	Runtime-driven	Evaluación continua nativa
Delegación	Priv. Mgmt + Reviews	Okta Delegation	mTLS roles	Delegación contextual
API Zero Trust	Front Door + Proxy	API Access Mgmt	mTLS + Attestation	CAEP policy-driven

CAPÍTULO 7: PROCESO DE IMPLEMENTACIÓN DE NHI GOVERNANCE (NHI-GA)

El modelo de Identidad como Infraestructura no puede quedarse en teoría; requiere una metodología clara para implementarse dentro de organizaciones complejas. El proceso NHI-GA propone un enfoque pragmático, gradual y completamente alineado a los principios de Zero Trust.

Su objetivo es ayudar a los equipos a identificar dónde empezar, cómo construir, cómo validar y cómo operar un sistema de identidad moderno que cubra tanto entidades humanas como no humanas.

7.1 POR QUÉ NO REPETIR EL MODELO IGA TRADICIONAL

Los modelos de IGA (Identity Governance & Administration) fueron diseñados para gobernar identidades humanas. Se basan en conceptos como onboarding, rol organizacional, matrices de acceso, certificaciones periódicas y flujos de aprobación.

Estos modelos funcionan bien para personas, pero fallan frente a workloads, APIs, pipelines, agentes de IA y sistemas de control. El volumen, velocidad, autonomía y naturaleza efímera de las identidades no humanas hacen inviable una réplica del modelo IGA.

Intentar aplicar IGA a NHI produce inventarios inservibles, políticas estáticas, procesos lentos, gobernanza superficial y zero trust incompleto.

NHI-GA es necesario porque el gobierno de identidades debe adaptarse al comportamiento de la tecnología moderna, no al de los modelos del pasado.

7.2 PUNTO DE INICIO: RIESGO + OBJETIVO EMPRESARIAL

El proceso NHI-GA comienza respondiendo dos preguntas:

- **¿Qué dominio genera mayor riesgo hoy?**
- **¿Qué objetivo empresarial debe protegerse o habilitarse?**

Si una empresa depende intensamente de APIs, ese es el punto de partida.
Si depende de IA, pipelines o workloads críticos, ese es el dominio.
Ejemplos:

- En banca: APIs de pagos, modelos de riesgo, workloads de core transaccional.
- En retail: servicios de inventario, integraciones logísticas, agentes de IA para forecasting.
- En manufactura: OT, actuadores, sensores y pipelines industriales.
- NHI-GA inicia donde el riesgo es tangible y donde el impacto al negocio es inmediato.

7.3 SELECCIÓN DEL DOMINIO CRÍTICO (APIS, PIPELINES, IA, OT, WORKLOADS)

Una vez identificado riesgo + objetivo, debe seleccionarse el dominio que recibirá el primer tratamiento NHI-GA.

Los dominios típicos son:

- **APIs**: expuestas, sensibles, dependientes de tokens y scopes.
- **Pipelines:** generan workloads, imágenes y artefactos.
- **IA**: agentes autónomos que consumen datos críticos.
- **OT**: dispositivos y procesos industriales que afectan seguridad física.
- **Workloads**: el motor central de la operación digital.

La selección no es técnica; es estratégica.
El dominio elegido determina el diseño del modelo inicial y genera aprendizajes que luego se expanden al resto de la organización.

7.4 DISEÑO DEL MODELO DE IDENTIDAD

Con el dominio definido, se procede a diseñar su modelo de identidad respondiendo:

- ¿Qué entidades existen?
- ¿Cuáles son humanas y cuáles no humanas?
- ¿Cuáles requieren identidad y cuáles no?
- ¿Qué atributos definen a cada identidad?
- ¿Qué validación debe realizarse antes de autorizar acciones?
- ¿Qué relación debe existir entre identidad y política?

El diseño incluye:

- Identidad declarada (Workload Identity, API Identity, IA Identity, etc.)
- Identidad runtime (Runtime Identity)
- Fuentes autoritativas
- Políticas iniciales
- Ciclo de vida
- Delegación humana

Este es el paso más importante del proceso; todo lo demás depende de que el modelo esté correctamente definido.

7.5 INTEGRACIÓN DEL PLANO ZERO TRUST

Una vez diseñada la identidad del dominio, debe integrarse el plano de autorización Zero Trust.
Esto significa:

- Evaluar identidad y atributos de forma continua.
- Validar integridad del runtime.
- Evaluar riesgo y señales contextuales.
- Aplicar reglas PBAC, ABAC o ReBAC según corresponda.
- Definir enforcement mediante PIP, PDP y PEP.
- Habilitar CAEP para reevaluación continua.

La autorización no se gestiona con roles estáticos:
es un motor dinámico basado en evidencia.

7.6 DELEGACIÓN HUMANA COMO PUENTE ESTRUCTURAL

Toda identidad no humana debe tener un dueño humano. En NHI-GA, la delegación humana establece:

- Quién es accountable de la acción.
- Qué límites tiene la identidad delegada.
- Qué atributos puede heredar.
- Cuándo debe revocarse la delegación.
- Cómo se audita su uso.

La delegación evita que las identidades técnicas operen sin supervisión y permite trazabilidad confiable para auditorías y cumplimiento.

7.7 DISCOVERY COMO VALIDACIÓN DEL MODELO (NO COMO PUNTO DE PARTIDA)

Tradicionalmente, los proyectos IAM comienzan con “descubrimiento” o inventarios.
En NHI-GA, eso sería un error.
Primero se diseña el modelo; luego se hace discovery para validar que el modelo representa la realidad, identificar desviaciones, ajustar políticas, detectar identidades invisibles,mapear entidades desconocidas.
El discovery es una prueba del modelo, no la base del modelo.

7.8 MATRIZ NHI-GA

La matriz NHI-GA organiza la gobernanza del dominio seleccionado.
Incluye:

- entidad,
- identidad,
- atributos,
- validación propia,
- autorizaciones requeridas
- riesgos asociados,
- delegación,
- señales de runtime,
- fuentes autoritativas.

La versión simplificada se utiliza para implementar rápido; la versión ampliada permite escalar a más dominios y mayor complejidad.

MATRIZ NHI-GA (Versión Simplificada)

Tipo de Entidad	Identidad que Proyecta	Fuente Autoritativa	Riesgo Primario	Validación Requerida	Delegación Humana
Work-load	Workload Identity	Architecture Repo	Ejecución no autorizada	Firma + hash + pipelineFirma +	Owner técnico
Runtime Instance	Runtime Identity	SPIRE / CA (SVID/mTLS)	Impersona-ción	Attestation	Delegación automática limitada
Pipeline CI/CD	Pipeline Identity	CI/CD System (SVID/mTLS)	Supply chain compromise	Firma + provenance	DevOps + Seguridad
API Client	API Client Identity	API Mgmt	Fraude API / abuso	OAuth + scopes	Owner de dominio
AI Agent	AI Agent Identity	AI Registry	Autonomía descontrolada	Modelo + dataset +	Delegación explícita
RDBMS/ Cluster	Service Identity	Service Catalog	Exfiltración	mTLS + firma	DBA + Seguridad
Server-less Func-tion	Workload/Ru ntime	Cloud Provider	Ejecución arbitraria	IAM roles + attestation	Equipo técnico
Sensor OT	Sensor Identity	OT Registry	Manipulación	Posture + key	OT Manager
Actua-dor OT	Actuator Identity	OT Registry	Daño físico	Secure channel + key	OT Manager
Secrets/ Keys	Key Identity	KMS/HSM	Movimiento lateral	Rotación + firma	Seguridad

Columnas que se pueden agregar según madurez

- **Señales Zero Trust relevantes**
- **Ciclo de vida completo (creación, operación, rotación, retiro)**
- **Prioridad NHI-GA basada en riesgo**
- **Controles Zero Trust aplicables (PBAC, ABAC, ReBAC, JIT, CAEP)**
- **Atributos de identidad requeridos**
- **Contexto del entorno (tenant, ambiente, ubicación)**
- **Integridad de supply chain (SLSA, in-toto)**
- **Datos sensibles involucrados**

La matriz puede crecer hasta convertirse en un tablero operativo. Considerando esta matriz, el proceso completo quedará como sigue:

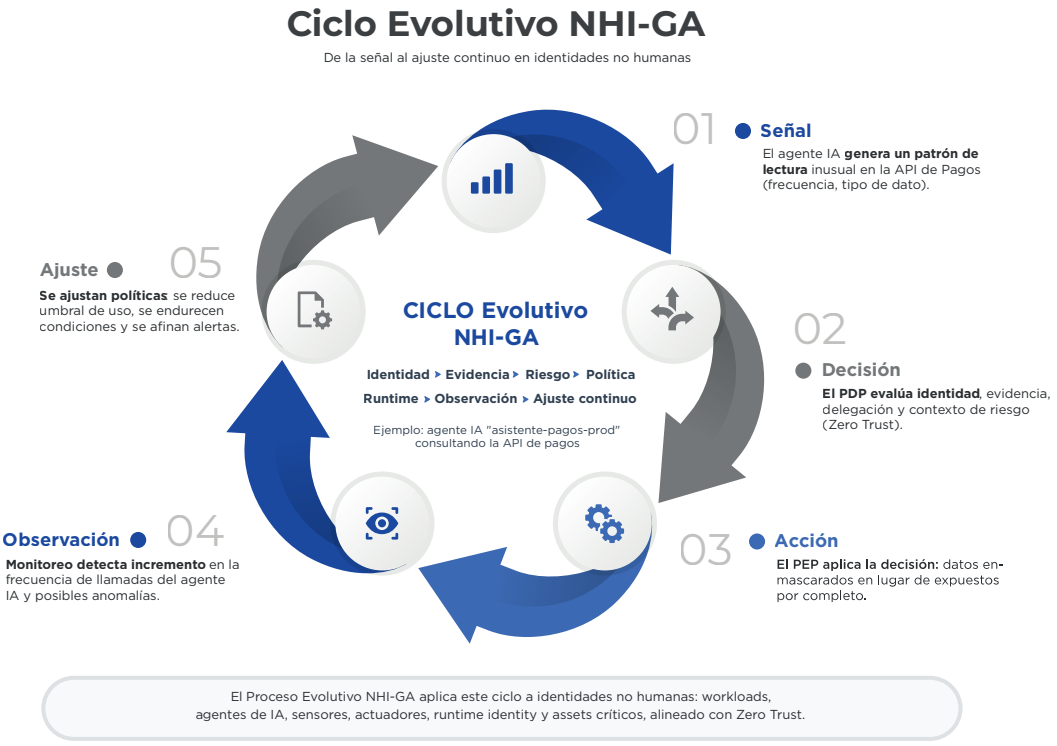
Proceso Evolutivo NHI-GA – Cadena de Valor

Ejemplo aplicado: el agente IA de pagos pasa por cada etapa del proceso evolutivo NHI-GA, permitiendo gobernarlo con identidad, evidencias, autorización Zero Trust y delegación correcta.

7.9 CICLO SEÑAL → DECISIÓN → ACCIÓN → OBSERVACIÓN → AJUSTE

NHI-GA opera como un ciclo continuo:
Señal: cambio en atributos, riesgo o contexto.
Decisión: el PDP evalúa políticas y determina autorización.
Acción: el PEP permite o bloquea.
Observación: se registra telemetría y comportamiento.
Ajuste: se actualizan políticas o atributos según lo observado.

Este ciclo convierte la arquitectura en un sistema adaptativo.



El Proceso Evolutivo NHI-GA aplica este ciclo a identidades no humanas: workloads, agentes de IA, sensores, actuadores, runtime identity y assets críticos, alineado con Zero Trust.

7.10 RESULTADO: ARQUITECTURA VIVA EMPRESARIAL

- Cuando NHI-GA está implementado:
- La organización tiene visibilidad completa de identidades humanas y no humanas.
- Zero Trust opera de forma continua y contextual.
- Las decisiones se basan en evidencia, no en configuraciones estáticas.
- La delegación humana es clara y auditable.
- El riesgo disminuye de manera estructural.
- La arquitectura se vuelve un sistema vivo, que evoluciona con el negocio.

NHI-GA habilita un gobierno moderno, preparado para IA, multicloud y automatización masiva.

CAPÍTULO 8: CONCLUSIÓN GENERAL

La transformación digital ha modificado la composición del universo operativo de las empresas. Lo que antes era un ecosistema dominado por identidades humanas ahora es un entorno dinámico, distribuido y mayoritariamente automatizado, donde workloads, servicios, APIs, pipelines y agentes de IA sostienen la operación. Frente a esta realidad, los modelos tradicionales de identidad —enfocados en usuarios, roles y flujos de aprobación— ya no son suficientes.

El modelo de **Identidad como Infraestructura** redefine la forma en que se gobierna el entorno digital, integrando validación continua, autorización basada en evidencia, delegación humana clara, Zero Trust dinámico y gobierno de ciclo de vida para identidades no humanas. Esta visión crea un marco capaz de sostener organizaciones modernas que dependen intensamente de tecnología y automatización.

8.1 EL FUTURO: MÁS MÁQUINAS QUE PERSONAS

Las organizaciones avanzan hacia una composición donde los workloads superan por cientos o miles a las identidades humanas, los agentes de IA toman decisiones y ejecutan acciones autónomas, las APIs se convierten en el principal mecanismo de interacción, los pipelines crean y mutan infraestructura sin intervención humana, los sistemas de control gobiernan automáticamente a otros sistemas.

En esta realidad, el crecimiento de identidades no humanas es exponencial, continuo, difícil de rastrear, altamente distribuido, operativo 24/7 y autónomo.

El riesgo ya no proviene de un empleado con acceso excesivo:
proviene de una identidad técnica sin validación, un token expuesto, un workload sin integridad o un agente de IA actuando fuera de límites.

El futuro exige un modelo donde la identidad sea universal, continua, verificable y gobernada como parte central de la arquitectura.

8.2 IDENTIDAD COMO INFRAESTRUCTURA = RESILIENCIA + GOBERNANZA + ZERO TRUST

La Identidad como Infraestructura une tres pilares que antes vivían separados:

1. Resiliencia: Porque permite saber con certeza qué entidad está actuando, con qué atributos, bajo qué condiciones y con qué integridad. Este conocimiento estructural reduce la superficie de ataque, previene brechas comunes y permite responder más rápido ante incidentes.

2. Gobernanza: Porque establece un marco claro donde cada identidad, humana o no humana, tiene dueño, atributos, políticas, ciclo de vida, validación, delegación y trazabilidad.
La gobernanza deja de ser un proceso estático para convertirse en una práctica viva.

3. Zero Trust Moderno

Porque el plano de autorización se vuelve dinámico: cada acción requiere evidencia, cada interacción se valida, cada identidad se evalúa continuamente. Zero Trust deja de ser conceptual para convertirse en operativo.

La combinación de estos tres elementos genera una infraestructura más segura, más auditable y más preparada para el futuro tecnológico.

8.3 CAPACIDADES HABILITADAS PARA EL NEGOCIO

Implementar Identidad como Infraestructura no solo mejora seguridad; habilita capacidades de negocio que antes eran difíciles o imposibles:

Automatización segura: Pipelines, agentes de IA y workloads pueden operar sin riesgo de pérdida de control.

Velocidad de innovación: Los equipos pueden desplegar cambios sin comprometer integridad o gobernanza.

Visibilidad completa: Cada entidad,humana y no humana, puede ser rastreada en tiempo real.

Reducción estructural del riesgo: Menos identidades invisibles, menos accesos fantasma, menos brechas por tokens, certificados o instancias no autorizadas.

Cumplimiento continuo: La trazabilidad de identidades técnicas facilita auditorías y cumplimiento regulatorio.

Arquitectura viva: La combinación de señales, decisiones, acciones y ajustes crea un sistema que se adapta al entorno sin intervención constante.

El futuro digital pertenece a las organizaciones que entiendan, gobiernen y controlen sus identidades no humanas con la misma precisión con la que protegen a sus usuarios. La identidad ya no es un componente del sistema: es la infraestructura que sostiene la operación, la resiliencia y la innovación del negocio.

3. Zero Trust Moderno

Porque el plano de autorización se vuelve dinámico: cada acción requiere evidencia, cada interacción se valida, cada identidad se evalúa continuamente. Zero Trust deja de ser conceptual para convertirse en operativo.

La combinación de estos tres elementos genera una infraestructura más segura, más auditable y más preparada para el futuro tecnológico.

8.3 CAPACIDADES HABILITADAS PARA EL NEGOCIO

Implementar Identidad como Infraestructura no solo mejora seguridad; habilita capacidades de negocio que antes eran difíciles o imposibles:

Automatización segura: Pipelines, agentes de IA y workloads pueden operar sin riesgo de pérdida de control.

Velocidad de innovación: Los equipos pueden desplegar cambios sin comprometer integridad o gobernanza.

Visibilidad completa: Cada entidad,humana y no humana, puede ser rastreada en tiempo real.

Reducción estructural del riesgo: Menos identidades invisibles, menos accesos fantasma, menos brechas por tokens, certificados o instancias no autorizadas.

Cumplimiento continuo: La trazabilidad de identidades técnicas facilita auditorías y cumplimiento regulatorio.

Arquitectura viva: La combinación de señales, decisiones, acciones y ajustes crea un sistema que se adapta al entorno sin intervención constante.

El futuro digital pertenece a las organizaciones que entiendan, gobiernen y controlen sus identidades no humanas con la misma precisión con la que protegen a sus usuarios. La identidad ya no es un componente del sistema: **es la infraestructura que sostiene la operación, la resiliencia y la innovación del negocio.**

La invitación es clara: comenzar hoy, en un dominio estratégico, con un modelo sólido de NHI Governance que habilite Zero Trust real, automatización segura y una arquitectura viva capaz de adaptarse a un entorno donde cada acción, cada servicio y cada agente debe validar quién es antes de actuar. **La oportunidad de fortalecer el futuro tecnológico de la organización está en sus manos; el momento para construirlo es ahora.**

ANEXOS

A.1 TÉRMINOS CLAVE

Identidad humana: Representación digital de una persona dentro de la organización, con atributos provenientes de HR, credenciales y factores de autenticación.

Identidad no humana (NHI): Representación digital de entidades que actúan sin intervención humana: workloads, servicios, APIs, sensores, actuadores y agentes de IA.

Workload Identity: Identidad declarada de un servicio; define qué proceso debe existir y bajo qué atributos y políticas.

Runtime Identity: Identidad de la instancia real en ejecución, validada mediante certificados efímeros, attestation y atributos contextuales.

Fuentes autoritativas: Sistemas o repositorios que contienen los atributos verdaderos de una identidad: HR, CI/CD, control-plane, repositorios de artefactos, manufactura, etc.

Zero Trust: Modelo donde cada acción requiere evidencia actualizada y ninguna entidad, humana o no humana, recibe confianza por defecto.

Delegación humana: Marco formal que define qué identidad técnica actúa en nombre de qué persona o equipo, bajo límites y políticas claras.

La invitación es clara: comenzar hoy, en un dominio estratégico, con un modelo sólido de NHI Governance que habilite Zero Trust real, automatización segura y una arquitectura viva capaz de adaptarse a un entorno donde cada acción, cada servicio y cada agente debe validar quién es antes de actuar. **La oportunidad de fortalecer el futuro tecnológico de la organización está en sus manos; el momento para construirlo es ahora.**

ANEXOS

A.1 TÉRMINOS CLAVE

Identidad humana: Representación digital de una persona dentro de la organización, con atributos provenientes de HR, credenciales y factores de autenticación.

Identidad no humana (NHI): Representación digital de entidades que actúan sin intervención humana: workloads, servicios, APIs, sensores, actuadores y agentes de IA.

Workload Identity: Identidad declarada de un servicio; define qué proceso debe existir y bajo qué atributos y políticas.

Runtime Identity: Identidad de la instancia real en ejecución, validada mediante certificados efímeros, attestation y atributos contextuales.

Fuentes autoritativas: Sistemas o repositorios que contienen los atributos verdaderos de una identidad: HR, CI/CD, control-plane, repositorios de artefactos, manufactura, etc.

Zero Trust: Modelo donde cada acción requiere evidencia actualizada y ninguna entidad, humana o no humana, recibe confianza por defecto.

Delegación humana: Marco formal que define qué identidad técnica actúa en nombre de qué persona o equipo, bajo límites y políticas claras.

A.2 EJEMPLOS DE POLÍTICAS PBAC

Política 1: Autorización basada en integridad (workloads)
Condición: Permitir acceso solo si el hash del binario coincide con la versión autorizada. Política PBAC:

```
permit action.read if
  workload.hash == approved.hash

  and workload.runtime_attestation == "valid"
```

Política 2: Acceso condicionado a riesgo del dispositivo
Condición: Usuario autenticado, pero dispositivo con postura desconocida → acceso restringido.

```
deny action.update if
  device.posture != "compliant"
```

Política 3: Límite de delegación para agentes IA

```
permit action.invoke_api if
  agent.identity == registered_agent
  and action.scope in allowed_scopes
  and human.delegate == active
```

Política 4: Autorización para APIs por contexto

```
permit api.transfer if
  api.client_risk < threshold
  and token.scope == "payments"
  and runtime_identity.integrity == "verified"
```

TEC360
Be Smart & Secure

@tec360cloud

@tec360cloud

info@tec360cloud.com

tec360cloud.com