PROPUESTA FUNDACIONAL 2025

GSN

Global Security Netguard

Una capa de confianza global

descentralizada para Internet

ABIERTO	PRIVADO	SOBERANO
Open source, sin propietario	Sin registro de metadatos	Sin gobierno central

Solo queremos que Internet sea más seguro para todos."
No buscamos control, beneficio ni reconocimiento.
"Ofrecemos esta arquitectura como un bien común digital.

Documento de dominio público · Licencia abierta sin restricciones

Versión 0.1 · 2026 · Diseñado por La Fábrica de Ideas · www.lafabricadeideas.info

Índice

01 EL PROBLEMA

Un mundo digital vulnerable y corruptible

Internet fue diseñado para la apertura y la interoperabilidad, no para la seguridad extrema. Décadas después de su creación, esa arquitectura original se ha vuelto insostenible frente a las amenazas actuales. Los parches sucesivos —contraseñas, doble factor, TLS, gestores de credenciales— no han resuelto el problema de fondo: **la ausencia de una capa de confianza distribuida, neutral y resistente a la corrupción.**

Phishing y suplantación de identidad	Los atacantes replican sitios y servicios con fidelidad creciente. El usuario no tiene forma fiable de verificar que el destino es legítimo.
Robo de credenciales y sesiones	Contraseñas, tokens y cookies son interceptados, filtrados o comprados en mercados clandestinos. La autenticación basada en secretos compartidos es estructuralmente débil.
Estafas con inteligencia artificial	Los deepfakes de voz e imagen hacen que la autenticación biométrica remota sea prácticamente inútil sin un ancla criptográfica de hardware.
Corrupción de la cadena de suministro	Software, firmware y hardware pueden ser comprometidos antes de llegar al usuario. Sin certificación física sellada, no hay garantía de integridad.
Vigilancia masiva y control centralizado	Los sistemas de identidad actuales concentran datos en manos de unos pocos actores —corporativos o estatales— creando vectores de control y abuso.

Los parches actuales son necesarios pero insuficientes. Se necesita un cambio de paradigma: una infraestructura nueva, diseñada desde la raíz con la confianza como objetivo único.

Documento fundacional de dominio público — Licencia abierta sin restricciones — 2026 — Diseñado por La Fábrica de Ideas · www.lafabricadeideas.info

02 POR QUÉ AHORA

El momento es crítico

Varios factores convergentes hacen que 2025 sea el momento idóneo para proponer una infraestructura de confianza global. No se trata solo de que los problemas sean graves: se trata de que las herramientas para resolverlos existen por primera vez.

IA generativa masiva	Los modelos de lenguaje e imagen permiten crear identidades falsas, voces clonadas y documentos sintéticos de calidad indistinguible. La ventana para establecer un estándar de confianza antes de que el caos sea irreversible se está cerrando.
Estándares maduros disponibles	WebAuthn/FIDO2, los Identificadores Descentralizados (DIDs) del W3C y las Credenciales Verificables son estándares ratificados, con implementaciones open source robustas. GSN no reinventa: integra y especializa.
Hardware criptográfico asequible	Chips con Secure Element certificados CC EAL6+ y soporte para criptografía post-cuántica están disponibles a escala industrial. El coste de un prototipo funcional es hoy inferior a 15 euros por dispositivo.
Crisis de confianza global	Ciudadanos, empresas y gobiernos han perdido la fe en la seguridad digital. Existe por primera vez una demanda social real de soluciones estructurales, no de más parches.

Documento fundacional de dominio público — Licencia abierta sin restricciones — 2026 — Diseñado por La Fábrica de Ideas · www.lafabricadeideas.info

03 LA SOLUCIÓN

GSN: una red de seguridad paralela y descentralizada

GSN no es un parche más sobre Internet. Es una red nueva, independiente, diseñada desde cero para un único propósito: verificar identidades y autorizar transacciones de forma segura, privada y resistente a la corrupción.

La idea central es la **separación de capas**: Internet (la red de datos) se ocupa del contenido. GSN (la red de seguridad) se ocupa exclusivamente de la autenticación y la validación. Ninguna interferencia entre ambas. Ningún punto único de fallo.

Componente	Función	Tecnología base
Autenticador GSN	Dispositivo físico del usuario. Genera y custodia la clave privada.	Secure Element CC EAL6+, nRF52840
Nodos de red GSN	Servidores distribuidos que verifican identidades (sin datos).	Malla descentralizada, protocolo PaP
Red de transporte	Comunicación redundante entre nodos.	Fibra terrestre + satélites LEO
Capa de identidad	Identificadores y credenciales verificables.	DIDs W3C + Verifiable Credentials
Consejo Técnico	Gobernanza del protocolo y certificación de hardware.	Modelo Linux Foundation / Apache

04 PRINCIPIOS

Principios fundamentales del protocolo

1. Separación de capas	GSN es una red paralela, no una extensión de Internet. La capa de seguridad y la capa de contenido operan de forma completamente independiente.
2. Descentralización geopolítica	Nodos desplegados por países, regiones y ciudades bajo soberanía local pero con protocolos comunes. No existe un punto único de fallo ni de control.
3. Hardware sellado e inmutable	Los dispositivos GSN se fabrican en instalaciones certificadas. Una vez sellados, cualquier intento de manipulación física destruye las claves criptográficas.
4. Validación binaria sin registro	La red solo responde preguntas de tipo sí/no: ¿está registrada esta identidad? ¿es válida esta transacción? No almacena contenido, metadatos ni historiales.
5. Identidad digital soberana	Cada entidad posee un hash de identidad único. No revela información personal, pero permite verificación criptográfica. El usuario es dueño de su identidad.
6. Privacidad por diseño	El seudonimato global es estructural: el DID es un hash, no un nombre. Las pruebas de conocimiento cero (ZKPs) permiten demostrar atributos sin revelarlos.
7. Resistencia a la corrupción	El 'poder' está distribuido. Ningún nodo, país o actor puede controlar la red. Un nodo comprometido puede ser aislado por consenso del resto.
8. Código abierto y auditable	El protocolo GSN es público, libre de patentes y auditable por cualquier persona o institución. La confianza se gana con transparencia, no con autoridad.

Documento fundacional de dominio público — Licencia abierta sin restricciones — 2026 — Diseñado por La Fábrica de Ideas · www.lafabricadeideas.info

05 ARQUITECTURA TÉCNICA

Arquitectura técnica del sistema

5.1 Autenticador GSN: el ancla de confianza

El autenticador es el dispositivo físico del usuario —llavero USB, tarjeta o chip— que genera y custodia la clave privada. Sus requisitos técnicos son:

- **Secure Element CC EAL6+:** Nivel de certificación utilizado en aplicaciones militares y gubernamentales. La clave privada nunca sale del chip.
- **FIPS 140-3 Level 3:** Certificación para módulos criptográficos de alta seguridad.
- **Sellado físico antimanipulación:** Resina epoxi + sensores de voltaje, temperatura y luz. Intrusión = borrado inmediato.
- **Criptografía post-cuántica:** Soporte para ML-KEM y ML-DSA (NIST PQC 2024). Implementación híbrida ECC/Dilithium.
- **Biometría local:** Huella dactilar y PIN procesados por el SE. Los datos biométricos nunca salen del dispositivo.

5.2 Red de nodos: malla de verificación

La red GSN no almacena un libro mayor de transacciones. Solo verifica la pertenencia y validez de las identidades mediante un protocolo de validación punto a punto (PaP) completamente sin estado (stateless):

- Topología en malla: cada nodo conecta con múltiples pares. Sin centro, sin jerarquía.
- Protocolo PaP: consulta binaria (válida/no válida) firmada criptográficamente por el nodo respondedor.
- Anclaje de confianza: el hash del Consejo Técnico GSN está precargado en cada dispositivo de fábrica.
- Red dual: fibra terrestre + satélites LEO para redundancia total ante cortes o ataques locales.
- Aislamiento de nodos maliciosos por sistema de reputación y veto colectivo.

5.3 Capa de identidad: DIDs y Credenciales Verificables

GSN utiliza los estándares del W3C para la identidad auto-soberana (SSI):

- **DID (did:gsn:)**: Identificador único global derivado de la clave pública. No revela información personal.
- **Verifiable Credentials**: Atributos firmados por entidades emisoras (gobiernos, notarios). El usuario decide qué presenta.
- **ZKPs (zk-STARKs)**: Pruebas de conocimiento cero. Demuestran atributos (ej. mayoría de edad) sin revelar el dato subyacente.

Documento fundacional de dominio público — Licencia abierta sin restricciones — 2026 — Diseñado por La Fábrica de Ideas · www.lafabricadeideas.info

5.4 Hardware de referencia para el prototipo

Componente	Opción	Nota
Microcontrolador	Nordic nRF52840	TrustZone CryptoCell-310, soporte OpenSK y CanoKey
Firmware base	OpenSK (Google, Rust)	FIDO2 robusto, código auditado
Alternativa NFC	CanoKey	Soporte NFC y versatilidad de credenciales
Placa prototipo	nRF52840 Dongle	~10-12 € por unidad
Certificación objetivo	CC EAL6+ / FIPS 140-3 L3	Para producción certificada

06 FLUJO DE AUTENTICACIÓN

Flujo completo de autenticación GSN

A continuación se describe el ciclo completo desde que el usuario activa el autenticador hasta que la transacción queda autorizada, sin que en ningún punto se exponga la clave privada ni se almacene un registro de la operación.

Fase 1

1

Arranque del autenticador

El dispositivo se conecta por USB/NFC. Solicita huella dactilar + PIN en bucle local. Solo tras validarlos activa el periférico y se presenta al sistema operativo. Sin autenticación local: sin función.

Fase 2

2

Solicitud del servicio (WebAuthn/FIDO2)

El sitio web o aplicación envía un desafío criptográfico al navegador, que lo transmite al autenticador vía protocolo CTAP.

Fase 3

3

Verificación del destino en la red GSN

El autenticador extrae el identificador del servicio (rpId) y consulta al nodo GSN más cercano: '¿Es válido este DID de servicio?' El nodo responde sí o no en milisegundos. Si no es válido, la operación se cancela.

Fase 4

4

Confirmación del usuario

El autenticador solicita el PIN del usuario para confirmar la acción específica. El PIN se coteja con la copia segura dentro del Secure Element. Nunca sale del dispositivo.

Fase 5

5

Firma y completación

Se genera la firma asimétrica con la clave privada (que nunca abandona el SE). El autenticador envía la respuesta firmada al navegador. La transacción queda autorizada. Ni GSN ni el dispositivo guardan registro de la operación.

En ningún paso la clave privada abandona el Secure Element. En ningún paso la red GSN almacena quién se comunicó con quién. La privacidad es estructural, no una promesa.

Documento fundacional de dominio público — Licencia abierta sin restricciones — 2026 — Diseñado por La Fábrica de Ideas · www.lafabricadeideas.info

07 PRIVACIDAD Y SEGURIDAD

Modelo de privacidad y seguridad

Privacidad desde el diseño (PbD)	En ningún punto se almacena un registro central de quién se comunicó con quién. El sistema de validación PaP es efímero por naturaleza: responde y olvida.
Seudonimato global	El DID del usuario es un hash derivado de su clave pública. Sin una Credencial Verificable que lo vincule a una identidad real, no hay forma de rastrear al individuo.
Resistencia a la corrupción de nodos	El poder está distribuido. La red puede aislar a un nodo malicioso mediante sistema de reputación y veto colectivo de los nodos pares.
Resistencia cuántica	El protocolo incorpora algoritmos post-cuánticos (ML-KEM, ML-DSA) desde el diseño, anticipando la amenaza de la computación cuántica sobre la criptografía actual.
Auditoría continua del hardware	Los servidores GSN tienen sellado físico y mecanismos de auditoría continua. Cualquier manipulación es detectable y el nodo queda automáticamente en cuarentena.
Sin dependencia de grandes tecnológicas	GSN es completamente descentralizado y de dominio público. Ninguna empresa, ningún gobierno y ningún actor privado puede apropiarse de la red.

Documento fundacional de dominio público — Licencia abierta sin restricciones — 2026 — Diseñado por La Fábrica de Ideas · www.lafabricadeideas.info

08 GOBERNANZA

Gobernanza: inspirada en el CERN y la Linux Foundation

La gobernanza de GSN no depende de ningún gobierno ni corporación. Se inspira en modelos demostrados de instituciones técnicas neutras que llevan décadas operando con éxito bajo los mismos principios: el **CERN**, la **Linux Foundation**, la **Apache Software Foundation** y el **W3C**.

Institución	Modelo que aporta a GSN
CERN	Infraestructura científica global financiada por estados sin control político. Gestión técnica independient
Linux Foundation	Protocolo open source gobernado por contribuidores técnicos. Ningún actor controla el proyecto. Finan
Apache Foundation	Meritocracia técnica. Decisiones por consenso de committers. Código siempre de dominio público.
W3C	Estándares web abiertos ratificados por consenso internacional. Ninguna empresa puede apropiarse de
ICANN (parcial)	Gestión descentralizada de recursos de Internet con representación multistakeholder (aunque mejorabl

Estructura de gobernanza propuesta para GSN

- **Consejo Técnico GSN:** Científicos e ingenieros elegidos por sus pares (academias, sociedades de ingeniería, organismos de estandarización). Define los protocolos, certifica fábricas de hardware y supervisa la infraestructura de satélites. Sin representación política ni corporativa.
- **Comunidades de desarrollo:** Cualquier persona o equipo puede contribuir al código open source. Las decisiones técnicas se toman por consenso de contribuidores, siguiendo el modelo Apache/Linux.
- **Financiación:** Organismos internacionales (ITU, UNESCO), fundaciones tecnológicas, universidades y contribuciones voluntarias de estados que deseen desplegar nodos. Sin dependencia de ningún actor único.
- **Transparencia total:** Protocolo abierto, auditable y libre de patentes. Todas las decisiones del Consejo Técnico son públicas. Cualquier implementación que cumpla el estándar puede participar en la red.

09 BENEFICIOS GLOBALES

Beneficios globales tangibles

Problema actual	Solución GSN
Phishing y sitios falsos	Imposible: GSN verifica el hash del destino antes de firmar cualquier operación.
Robo de contraseñas o cookies	Inútil: sin el dispositivo físico GSN no existe autenticación posible.
Suplantación por deepfake	La clave privada está sellada en hardware. No se puede clonar ni duplicar.
Corrupción de administradores	Los servidores GSN tienen sellado físico y auditoría continua automatizada.
Vigilancia masiva de transacciones	GSN no registra metadatos. Solo responde sí/no de forma efímera.
Ataques a la cadena de suministro	Fábricas certificadas y hardware sellado impiden firmware malicioso.
Dependencia de grandes tecnológicas	GSN es descentralizado y de dominio público. Sin propietario, sin monopolio.
Exclusión digital	Cualquier país o comunidad puede desplegar nodos bajo los estándares abiertos
Estafas con IA	La autenticación no depende de biometría remota, sino de hardware físico infalsi

Paz mental, confianza y seguridad digital para ciudadanos, empresas, bancos, prensa y gobiernos. Un mundo donde las transacciones electrónicas son tan seguras y verificables como una firma notarial presencial.

10 HOJA DE RUTA

Hoja de ruta técnica

Fase 0	0 – 3 meses	**Documentación y semilla**

• Publicar la especificación formal del protocolo GSN v0.1. • Crear el repositorio público en GitHub bajo licencia abierta. • Publicar el Libro Blanco y convocar a los primeros contribuidores. • Contactar con comunidades FIDO Alliance, IETF, W3C y universidades.

Fase 1	3 – 12 meses	**Prototipo de laboratorio**

• Implementar el firmware del autenticador (OpenSK + lógica GSN). • Desarrollar el software de nodo GSN con API de registro y consulta PaP. • Integrar la capa DID en el autenticador. • Desplegar un clúster de prueba con 10-20 nodos voluntarios en distintos países.

Fase 2	12 – 24 meses	**Red de pruebas cerrada**

• Expandir a 50+ nodos distribuidos en distintos continentes. • Implementar el protocolo de consenso entre nodos. • Añadir la capa de Credenciales Verificables y ZKPs. • Realizar auditorías de seguridad independientes. • Refinar el diseño del hardware hacia certificación CC EAL6+.

Fase 3	24 – 36 meses	**Piloto público y estandarización**

• Lanzar la red de pruebas pública GSN. • Certificar la primera fábrica de hardware (candidatas: Suiza, Singapur). • Iniciar el proceso de estandarización en IETF/ISO. • Explorar integración con redes satelitales LEO (IRIS², Rivada).

Fase 4	3 – 7 años	**Despliegue global y madurez**

• Desplegar nodos en más de 100 países. • Adopción por bancos, gobiernos y plataformas (coexistiendo con sistemas actuales). • GSN se convierte en estándar de facto para autenticación de alto valor. • Investigación continua en hardware post-cuántico y nuevas formas de sellado.

11 CÓMO CONTRIBUIR

Cómo contribuir a GSN

GSN es un regalo a la humanidad digital. No buscamos reconocimiento, beneficio ni control. Buscamos personas e instituciones que quieran construir este bien común. Estas son las formas de contribuir:

Desarrolladores e ingenieros

Implementar el firmware del autenticador, el software de nodo, los protocolos de red y la capa de identidad. El repositorio estará abierto en GitHub desde el primer día.

github.com/gsn-protocol (propuesto)

Investigadores y académicos

Auditar el protocolo, proponer mejoras, investigar en criptografía post-cuántica, privacidad y gobernanza descentralizada. Publicar papers que respalden la base técnica.

Contacto: grupos de investigación en seguridad y criptografía

Comunidades open source

FIDO Alliance, IETF, W3C, OpenSK, CanoKey, y cualquier proyecto afín. GSN está diseñado para integrarse y colaborar, no para competir.

Propuesta de colaboración disponible en el repositorio

Organismos internacionales e instituciones

UNESCO, ITU, fundaciones tecnológicas, universidades y estados que quieran desplegar nodos o financiar el desarrollo de la infraestructura.

Propuesta formal disponible bajo petición

Ciudadanos y divulgadores

Explicar la importancia de GSN, traducir documentos, organizar comunidades locales, testear los primeros prototipos cuando estén disponibles.

Foros y canales de comunicación abiertos desde la Fase 0

12 LLAMADA A LA ACCIÓN

Llamada a la acción

GSN no es una utopía. Es una necesidad técnica, económica y social. El estado actual de Internet es insostenible. La confianza digital se ha roto. Los parches ya no funcionan.

Este documento es la semilla. No pertenece a nadie y pertenece a todos. Ha sido redactado por arquitectos conceptuales que no tienen interés en dirigir el proyecto, poseerlo ni beneficiarse de él. Solo en que exista.

Lo que proponemos es una **infraestructura nueva, limpia, diseñada desde la raíz con la seguridad y la privacidad como únicos objetivos**, gobernada por quienes la construyen y usada libremente por toda la humanidad.

"Una infraestructura de confianza para la humanidad digital.

Sin dueño. Sin fronteras. Sin agenda oculta.

Solo código, hardware y voluntad colectiva."

Próximos pasos inmediatos

- Publicar este documento en comunidades open source (FIDO Alliance, IETF, GitHub).
- Redactar la especificación técnica formal del protocolo GSN v0.1.
- Crear el repositorio público y convocar a los primeros contribuidores.
- Contactar con organismos internacionales (ITU, UNESCO) para explorar respaldo institucional.
- Establecer los canales de comunicación abiertos (foro, lista de correo, chat).

Global Security Netguard — GSN

Versión 0.1 · 2026 · Dominio público · Licencia abierta sin restricciones

Diseñado por La Fábrica de Ideas · www.lafabricadeideas.info