— ESEA™ · EXTERNAL SECURITY EXPOSURE ASSESSMENT

Conocé y Gestioná la Exposición Digital de tu organización

Framework Propietario.-

ANÁLISIS PASIVO · NO INTRUSIVO · LOW NOISE · ONPREMISE & CLOUD · FRAMEWORK PROPIETARIO · VISIÓN ATACANTE

— POR QUÉ ESEA?

Beneficios del Assessment

Una visión externa, objetiva y no intrusiva de su Superficie Digital.

Resultados en <5 días

Desde el kickoff hasta la entrega del Informe en menos de 5 días hábiles. Sin coordinación interna ni instalación de software.

Visibilidad Integral de la Superficie de Ataque

Estado completo y actualizado de todos los activos digitales expuestos desde la perspectiva de un atacante externo.

Identificación Temprana de Riesgos

Detección anticipada de riesgos operativos y tecnológicos antes de que se conviertan en incidentes de seguridad reales.

Priorización Inteligente de Riesgos

Clasificación y ordenamiento de hallazgos por impacto potencial real, permitiendo focalizar recursos en lo que más importa.

Scoring con Framework Propietario

Índice Global ponderado con metodología ESEA™, Drivers de Riesgo, Impacto, Probabilidad, Exposición y Findings (trazable y auditable).

Shadow IT Detectado

Identificación de activos digitales sin inventario, sin aprobación y sin control que generan exposición invisible para la organización.

Detección de Activos Expuestos

Mapeo exhaustivo de servicios, puertos, aplicaciones e infraestructura accesible desde Internet sin autenticación.

Mejora Continua de la Postura de Seguridad

Cada engagement genera una línea de base medible que permite comparar evolución y demostrar progreso concreto en el tiempo.

Gobernanza Tecnológica y de Ciberseguridad

Fortalecimiento del gobierno de seguridad con evidencia objetiva, métricas ejecutivas y soporte para auditorías regulatorias.

9	<5d	3	0	100%
CAPAS	ENTREGA	ENTREGABLES	AGENTES	PASIVO

— PRODUCTO FLAGSHIP

ESEA — ¿QUÉ ES Y CÓMO FUNCIONA?

ESEA™ es el framework propietario de Genoma IT para medir y gobernar el **Riesgo de la Exposición Digital** en tu organización.

— METODOLOGÍA · 9 CAPAS

Framework ESEA™ — Cobertura en 9 Capas de Análisis

C1 **Dominios y Subdominios** Enumeración completa de superficie DNS visible externamente.	C2 **Network Exposure** IPs públicas, puertos expuestos, Shadow IT Matrix.	C3 **Services Enumeration** Servicios, acceso remoto, legacy y superficies administrativas.
C4 **Criptografía SSL/TLS** Certificados, protocolos, autofirmados, wildcards y validez.	C5 **OS Fingerprints** Identificación pasiva de sistemas operativos y vendors.	C6 **Web Applications** Stack tecnológico, WAF, CMS, VPN portals y endpoints.
C7 **Hardening** Antiphishing SPF/DMARC, cabeceras HTTP y configuraciones.	C8 **IAM / Identidades** Portales, VPN surfaces, paneles ICS/SCADA y exposición.	C9 **Supply Chain** Dependencias externas, proveedores, CDN y APIs de terceros.

— PROCESO DE TRABAJO

01	02	03	04	05
Kickoff Definición de scope y dominio raíz	**Enumeración** Recolección pasiva en 9 capas	**Análisis** Correlación y scoring ESEA™	**Priorización** Findings por severidad e impacto	**Entrega** 3 documentos + plan de acción

SCORING EJECUTIVO · ESTADOS

BLINDADO	CONTROLADO	VIGILADO	EXPUESTO	CRÍTICO
0–20%	21–40%	41–60%	61–80%	81–100%

— ¿QUÉ ANALIZA?

- **Superficie Digital Expuesta** — dominios, subdominios, IPs y servicios visibles desde Internet.
- **Aplicaciones y Servicios** accesibles públicamente sin autenticación.
- **Configuraciones Débiles** y tecnologías obsoletas o fuera de soporte.
- **Dependencias Externas** — Supply Chain Digital, Terceros conectados y CDNs.

— ¿CÓMO LO HACE?

01 **Scoring Ejecutivo**
Índice Global Ponderado con Drivers de Riesgo, Impacto, Probabilidad, Exposición y Findings.

02 **Enumeración Técnica Estructurada**
Mapeo de activos en 9 capas de cobertura sin acceso interno ni instalación de agentes.

03 **Análisis de Exposición**
Correlación de hallazgos y clasificación por severidad y riesgo real con evidencia objetiva y trazable.

— CASOS DE USO · INDUSTRIAS Y SECTORES

ESEA™ responde a los desafíos reales de cada sector

— ¿PARA QUIÉN?

- Bancos & Fintech
- Aseguradoras
- Mercado de Capitales
- SaaS / eCommerce
- Industria & Energía
- Gobierno

— SOPORTE PARA AUDITORÍAS Y GESTIÓN EJECUTIVA

Alineado a Marcos Normativos y Regulatorios

ISO 27.000 · BCRA · SSN · SOX · CNV

Bancos, Fintech y Agencias de Cambio

BCRA · CNV regulados

Evaluación de portales de banca online, plataformas de pagos y sistemas de identidad accesibles desde Internet. Soporte para auditorías BCRA y CNV con evidencia objetiva y métricas ejecutivas trazables.

BCRA COMPLIANCE · IDENTITY SURFACE · ANTIPHISHING

Industria y Energía

OT/IT convergence · ICS/SCADA

Detección de interfaces de control industrial y automatización accesibles pasivamente desde Internet. Evaluación de visibilidad pública de sistemas OT/IT que concentran riesgo operativo crítico.

ICS EXPOSURE · ADMIN PANELS · SHADOW IT OT

Aseguradoras y SSN

SSN · Compliance regulatorio

Análisis de portales de clientes, plataformas de siniestros y sistemas de gestión accesibles externamente. Generación de evidencia auditada para cumplimiento SSN y marcos de gobierno de riesgo tecnológico.

SSN COMPLIANCE · CLIENT PORTAL · RISK SCORING

Grandes Organizaciones & SaaS

Multi-dominio · Supply Chain digital

Evaluación de entornos multi-dominio con alta exposición de aplicaciones web, dependencias externas y activos cloud. Detección de shadow IT, activos huérfanos y misconfiguraciones en infraestructuras complejas.

MULTI-DOMAIN · SUPPLY CHAIN · CLOUD RISK

Gobierno y Organismos Públicos

Infraestructura crítica · Cumplimiento

Análisis de la exposición digital de portales ciudadanos, sistemas de gestión pública y plataformas de datos sensibles. Soporte para auditorías de seguridad de infraestructura crítica del Estado.

INFRA CRÍTICA · PORTALES CIUDADANOS · DATOS PÚBLICOS

Mercado de Capitales · CNV

Compliance CNV · Alta regulación

Evaluación de plataformas de trading, gestoras de fondos y brokers regulados por CNV. Evidencia de madurez digital para procesos de habilitación regulatoria y due diligence institucional.

CNV COMPLIANCE · TRADING PLATFORMS · DUE DILIGENCE

— CADA ENGAGEMENT INCLUYE

x3 DOCs ENTREGABLES

Documentación lista para Directorio, Auditoría y Equipos Técnicos.

01 — EJECUTIVO

Resumen Ejecutivo

Visión consolidada de la Postura de Exposición y Riesgo Digital para Dirección, CIO y CTO. Incluye DashBoard Consolidado, Conclusiones Estratégicas y Oportunidades de Mejora prioritarias.

VOLUMEN DEL DOC

17 Páginas

CONTENIDO DEL DOCUMENTO

- Estado Identificado
- Análisis de Riesgos
- Madurez
- FODA
- Prioridades Estratégicas
- Conclusión Final

02 — DASHBOARD

Dashboard

Herramienta visual para explorar los resultados Resumidos del Assessment. Permite trazabilidad, tendencias, análisis en profundidad y seguimiento continuo de la evolución de Riesgo, Exposición, Probabilidad, Impacto y Findings.

VOLUMEN DEL DOC

15 Páginas

VISTAS INCLUIDAS

- Scoring Global
- Risk Operational Matrix
- Drivers
- Superficie de Ataque
- Heat Map
- Findings Management
- Top 15 Risks
- Layer Stack 01/09
- Action Plan

03 — TÉCNICO

Anexo Técnico

Documento para equipos de Infraestructura, Redes, Seguridad y Arquitectura. Contiene detalle de activos detectados, evidencias, hallazgos, configuraciones observadas y recomendaciones de remediación.

VOLUMEN DEL DOC

220 Páginas

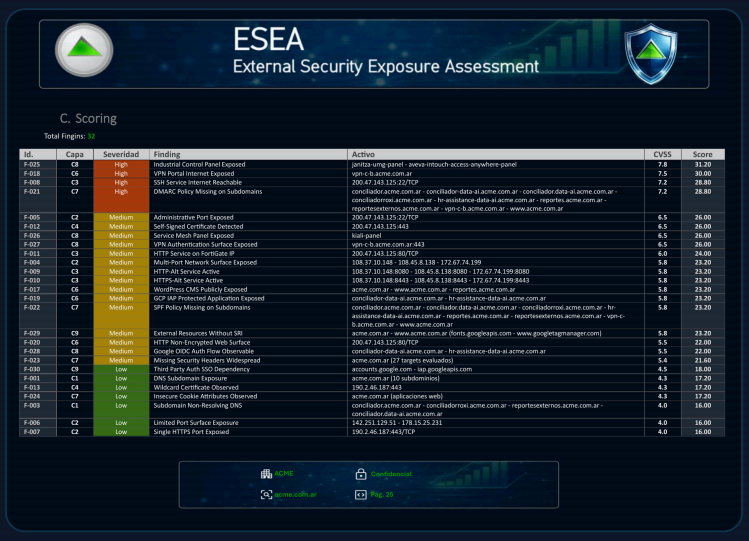
CONTENIDO TÉCNICO

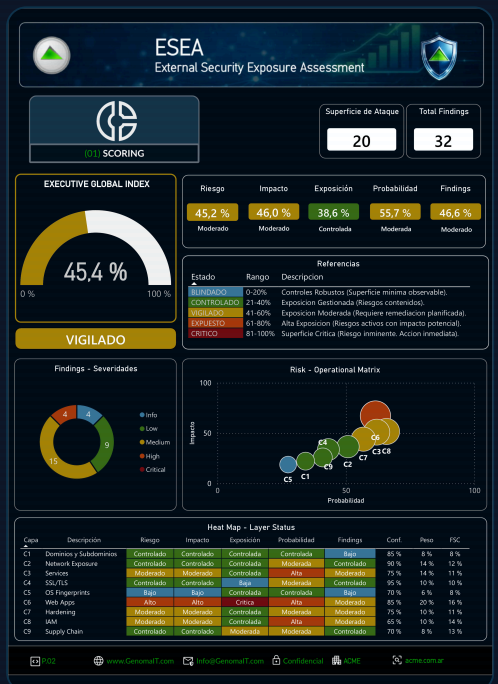
- Findings Detallados
- FODA por Capa
- Plan de Acción Detallado
- Attack Surface Detallada
- Evidencias Técnicas
- Framework

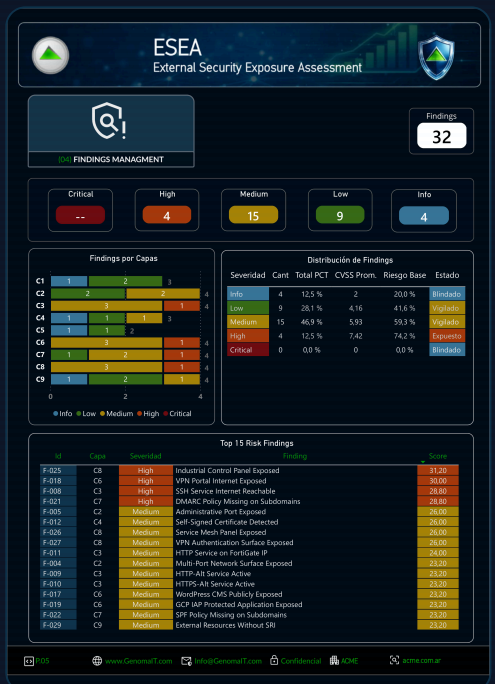
— CADA ENGAGEMENT INCLUYE

x3 DOCs ENTREGABLES

Documentación lista para Directorio, Auditoría y Equipos Técnicos.







— MODALIDADES DEL SERVICIO

Elige la modalidad que mejor se adapta a las necesidades de tu organización

CARACTERÍSTICA	ASSESSMENT SPOT / PUNTUAL Evaluación en un momento específico	ASSESSMENT + SEGUIMIENTO Evaluaciones periódicas para medir la evolución	CONTINUOUS ATTACK SURFACE MANAGEMENT (CASM) Monitoreo continuo 24/7 de la superficie digital
Assessment completo de la superficie de exposición	✓	✓	✓
Índice Global de Exposición (Scoring Ejecutivo)	✓	✓	✓
Executive Summary	✓	✓	✓
Dashboard Ejecutivo (Power BI)	✓	✓	✓
Anexo Técnico con evidencias y recomendaciones	✓	✓	✓
Presentación Ejecutiva de resultados	✓	✓	✓
Frecuencia de evaluación	Única	Mensual / Trimestral / Semestral	**Continua (24/7)**
Comparación histórica de resultados	✗	✓	✓
Alertas de nuevos activos y cambios	✗	Según frecuencia	✓
Monitoreo continuo de la superficie	✗	Según frecuencia	✓
Detección temprana de riesgos emergentes	✗	✓	✓
Seguimiento del Plan de Acción	Incluye inicial	✓	✓
Soporte y consultas	Por el proyecto	Continuo	Continuo

Ideal para: Conocer el estado actual

Conocer el estado actual de la postura de seguridad con una foto puntual de la exposición digital.

Ideal para: Medir y mejorar

Medir y mejorar la postura de seguridad en el tiempo, con evaluaciones periódicas y comparativa histórica.

Ideal para: Proteger de forma continua

Proteger, detectar y responder de forma continua ante cambios en la Superficie de Ataque expuesta.

— POSICIONAMIENTO COMPETITIVO

¿Por qué ESEA™ es diferente a los enfoques tradicionales de seguridad?

CRITERIO	ESEA™ · GENOMA IT	PENTEST TRADICIONAL	ESCÁNER AUTOMATIZADO
Framework propietario con scoring ejecutivo	✓	✗	✗
Visión de atacante externo pasivo (no intrusivo)	✓	✓	Parcial
Entregables ejecutivos para Dirección / Auditoría	✓	✗	✗
Dashboard Power BI con trazabilidad completa	✓	✗	✗
Resultados en menos de 5 días hábiles	✓	✗	✓
Sin agentes ni acceso interno requerido	✓	✗	Parcial
Plan remediación corto / mediano / estratégico	✓	Parcial	✗
Alineado a ISO 27000, NIST CSF, BCRA, SSN, CNV	✓	Parcial	✗
Cobertura Supply Chain Digital (9 capas)	✓	✗	✗
Soporte en Auditorías Externas y Regulatorias	✓	Limitado	✗

Visión Atacante

Analizamos exactamente lo que puede ver un atacante externo real — sin coordinar con el cliente ni alertar sus sistemas.

Framework Propietario

Scoring propio, índices ponderados y estados de referencia únicos — no replicables por escáneres genéricos.

Tres niveles de entregables

Resumen Ejecutivo para Dirección, Dashboard interactivo para gestión, y Anexo Técnico detallado para IT — un solo engagement cubre los tres niveles.

— QUIENES SOMOS?

Genoma IT

Firma especializada en Gobierno y Exposición Digital para organizaciones Industriales y Reguladas.

Genoma IT es una firma de consultoría especializada en **Gobierno y Exposición Digital** para organizaciones industriales y reguladas. Combinamos visión estratégica, rigor técnico y enfoque de negocio para transformar la exposición digital en una variable **medible, gestionable y gobernable**.

ESEA™ surge de más de **20 años de experiencia** liderando áreas de Infraestructura, Seguridad y Operaciones IT en entornos críticos y regulados — incluyendo multinacionales, empresas de energía, manufactura, agroindustria y servicios profesionales de primer nivel.

MISIÓN

Acompañar a las empresas en la protección de sus Activos Digitales, transformando la exposición en inteligencia accionable para la Dirección.

VALORES

- Integridad
- Confidencialidad
- Compromiso
- Ética
- Transparencia
- Metodología
- Profesionalismo

Ing. Jorge H. Carnero

Founder · Genoma IT

- Ing. en Sistemas (UAI)
- MBA Máster en Gestión Empresaria (UNR)
- Posgrado en Ciberseguridad y Auditoría de Sistemas (I-Sec)
- Posgrado en Gerencia de Sistemas - Tecnologpia y Seguridad Informática (ENFL)
- Posgrado en Gestión de Proyectos PMP (ENFL)
- Especialización en Telecomunicaciones - CCNA Cisco Systems (Proydesa)

BIO

Lidero estrategias de Tecnología, Ciberseguridad y Transformación Digital para organizaciones que requieren excelencia operativa, resiliencia tecnológica y gobierno efectivo de TI.

Con más de 20 años de experiencia en posiciones Ejecutivas y Gerenciales de compañías Multinacionales, Energía, Industria, Agroindustria y Servicios Profesionales, acompaño a directorios y ejecutivos en la toma de decisiones críticas vinculadas a Riesgo, Continuidad Operativa, Seguridad de la Información e Innovación Tecnológica.

EXPERIENCIA

- **Genoma IT** | Founder - Cibersegurity
- **fyo - Grupo IRSA Cresud** | Head of Infraestructure - IT
- **Electrolux ARG.** | Jefe de Infraestrutura & BP Proyectos IT - LATAM
- **CAMMESA** | Analista de Ciberseguridad
- **AES Corp.** | Analista de Infraestructura
- **COA Consultora** | Responsable de Tecnologia y Ciberseguridad
- **Universidad Abierta Interamericana** | Docente de Cátedra

Linkedin.com/in/JorgeCarnero

— PORTFOLIO DE SERVICIOS

Más allá de la Superficie:

Consultoría Integral de Ciberseguridad y Tecnología.

ISO 27.000 — Implementación y Lineamientos

Seguridad de la información alineada a estándares internacionales.

Acompañamiento en la implementación de controles ISO 27000: políticas, gestión de activos, control de accesos y seguridad operacional. Gestión de incidentes, continuidad del negocio y alineamiento con marcos regulatorios internacionales y locales.

- Políticas de Seguridad
- Gestión de Incidentes
- Continuidad Operativa

Diagnóstico de Tecnología y Seguridad

Conocé tu riesgo real antes de que sea un problema.

Relevamiento y evaluación integral del estado de madurez tecnológica, controles de seguridad y dependencias críticas de personal. Base sólida para un plan de seguridad ejecutable.

- Claridad para Dirección
- Priorización
- Reducción de Riesgo

IA + Automatización de Procesos

Eficiencia operativa, seguridad y reducción de costos.

Implementación de soluciones de inteligencia artificial y automatización para eliminar errores, ganar trazabilidad y liberar recursos humanos de tareas repetitivas de bajo valor.

- Reducción de Costos
- Trazabilidad
- Eficiencia Operativa

Monitoreo & Disponibilidad de Servicios IT

Dashboard y alertas antes de que el negocio se detenga.

Monitoreo proactivo de la infraestructura IT con dashboards en tiempo real y alertas tempranas. Reduce tiempos de caída y mejora la experiencia de usuarios y clientes.

- Detección Temprana
- Alta Disponibilidad
- Decisiones Objetivas

Plan de Contingencia y Continuidad del Negocio

Preparados para responder, recuperarse y seguir operando.

Diseño de planes de respuesta y continuidad con BIA (Business Impact Analysis). Evita la improvisación ante incidentes y reduce el tiempo de inactividad operativa.

- BIA
- Recuperación Rápida
- Confianza para Dirección

Auditorías IT, SOX y CNV

Cumplimiento normativo sin estrés ni improvisación.

Revisión de controles, documentación técnica y funcional para cumplimiento de SOX, CNV y marcos normativos locales. Reduce la exposición legal y la dependencia de personal clave.

- SOX
- CNV
- Controles Formales
- Documentación Técnica

— HABLEMOS

Contacto Directo

Escribinos y coordinamos el kickoff.

¿Sabés lo que ve un Atacante de tu organización?

En menos de 5 días Genoma IT te muestra tu superficie de ataque real. Sin instalar nada. Sin acceso a tus sistemas.
Solo una dirección de dominio y nuestra metodología de 9 capas.

EMAIL
Info@GenomaIT.com

WHATSAPP
+549 341 5027 547

WEB
www.GenomaIT.com