



INFORME DE EVALUACIÓN

Ciberseguridad Empresarial

WagnerSolutionsAI

Tecnología · Chile

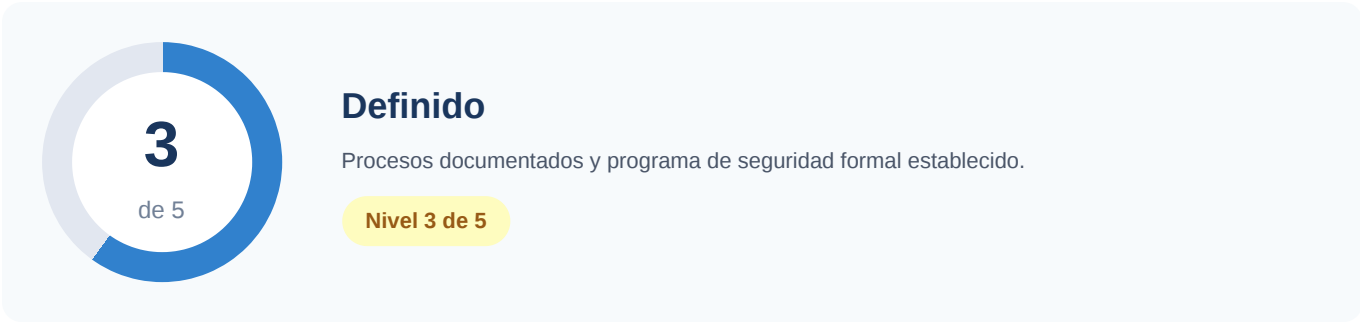
Preparado para: Sebastián Wagner · CTO

Fecha: 19 de enero de 2026

Resumen Ejecutivo

WagnerSolutionsAI ha establecido un programa formal de seguridad. Fortalezas: políticas de privacidad documentadas; auditorías trimestrales. Áreas de mejora: sin protección anti-phishing; sin monitoreo de credenciales comprometidas.

Nivel de Madurez General



Puntuación por Función NIST



Perfil de la Empresa

EMPRESA WagnerSolutionsAI	INDUSTRIA Tecnología	PAÍS Chile
TAMAÑO Micro (1-10)	INFRAESTRUCTURA híbrida	CLOUD No especificado

Hallazgos Principales

Brechas Identificadas

-  Sin protección anti-phishing
-  Sin monitoreo de credenciales comprometidas
-  Respaldos solo trimestrales

Fortalezas Detectadas

-  Políticas de privacidad documentadas
-  Auditorías trimestrales
-  MFA implementado
-  Plan de respuesta a incidentes

Soluciones Recomendadas

1

BullPhish ID

Entrenamiento y simulaciones de phishing.

2

Dark Web ID

Monitoreo de credenciales comprometidas en la dark web.

3

SaaS Protection

Solución recomendada basada en el assessment.

Evaluación Detallada por Función NIST

	IDENTIFICAR Gestión de activos, riesgos y gobernanza	3/5 Puntuación
Hallazgos: Inventario documentado. Recomendaciones: Implementar gestión de activos y evaluación de vulnerabilidades.		
	PROTEGER Controles de acceso y seguridad de datos	3/5 Puntuación
Hallazgos: Fortalezas: MFA implementado. Áreas de mejora: Sin protección anti-phishing. Recomendaciones: Fortalecer MFA, programa de concientización y políticas de acceso.		
	DETECTAR Monitoreo continuo y detección de amenazas	2/5 Puntuación
Hallazgos: Áreas de mejora: Sin monitoreo de credenciales comprometidas. Recomendaciones: Implementar monitoreo continuo y considerar SOC gestionado.		

**RESPONDER**

Planificación y gestión de incidentes

3/5

Puntuación

Hallazgos:

Fortalezas: Plan de respuesta a incidentes.

Recomendaciones:

Documentar plan de respuesta y realizar simulacros.

**RECUPERAR**

Respaldo, continuidad y resiliencia

2/5

Puntuación

Hallazgos:

Áreas de mejora: Respaldos solo trimestrales.

Recomendaciones:

Implementar respaldo híbrido, definir RTO/RPO y probar recuperación.

Plan de Acción Recomendado

1**Corto Plazo (0-30 días)**

Implementar monitoreo de activos críticos y alertas básicas.

2**Mediano Plazo (30-90 días)**

Implementar BullPhish ID y Dark Web ID. Establecer métricas de seguridad.

3**Largo Plazo (90+ días)**

Optimizar procesos, implementar automatización y desarrollar threat hunting.

¿Listo para fortalecer tu seguridad?

Nuestro equipo de especialistas está disponible para ayudarte a implementar estas recomendaciones.



WEB

www.nuvo.pe

EMAIL

contacto@nuvo.pe

TELÉFONO

+51 1 234 5678