CYBERBROT

INFORME ESTRATÉGICO CYBERBROT · INFORME EJECUTIVO PARA EL DIRECTORIO

Shadow AI y agentes.

Gobernanza, riesgos y mitigación en el uso de inteligencia artificial.

- SHADOW AI Y AGENTES
- CHILE
- SEPTIEMBRE 2026
- LEYES 21.663 Y 21.719
- ISO/IEC 42001

01 Resumen ejecutivo: el imperativo estratégico ante el boom de la IA

02 Vector 1: Shadow AI y gobierno de datos

03 Vector 2: agentes AI autónomos en producción y control operacional

04 Estrategias de solución: hoja de ruta diferenciada

05 Conclusión: llamado a la acción para el Directorio

01

RESUMEN EJECUTIVO

El imperativo estratégico ante el boom de la IA.

La adopción de la Inteligencia Artificial (IA) en sus distintas modalidades se ha posicionado como un imperativo para mantener la competitividad del negocio. Sin embargo, su despliegue expone a la organización a **dos vectores de riesgo estructuralmente distintos** que exigen la atención inmediata del Directorio:

1. La **fuga de datos sensibles** mediante el uso no autorizado de IA pública (Shadow AI).
2. El **riesgo operacional** derivado de la ejecución autónoma de agentes AI en entornos productivos.

En el contexto regulatorio chileno, marcado por la **Ley 21.663** (Ley Marco de Ciberseguridad) y la **Ley 21.719** (Protección de Datos Personales), abordar ambos frentes mediante un marco de gobernanza diferenciado no es solo un requerimiento de cumplimiento, sino la vía para proteger el patrimonio y la continuidad operacional de la compañía.

02

VECTOR 1

Shadow AI y gobierno de datos: exposición por uso no autorizado.

Naturaleza del riesgo

Ocurre cuando los colaboradores emplean plataformas y herramientas públicas de IA generativa sin autorización ni supervisión de las áreas de TI y Ciberseguridad, introduciendo documentación sensible, estados financieros, proyectos estratégicos o bases de datos de clientes para optimizar sus tareas diarias.

Impacto legal, regulatorio y soberanía de datos

Al ingresar información confidencial en motores abiertos, la compañía pierde la **Soberanía de Datos**, ya que los contenidos pasan a alimentar modelos de terceros. Las sanciones asociadas a este vector de fuga de información comprenden:

- **Ley 21.719 (Protección de Datos Personales):** Sanciones por negligencia o filtración de datos de clientes y secretos comerciales que alcanzan hasta 20.000 UTM.
- **Ley 21.663 (ANCI):** Para Operadores de Importancia Vital (OIV) y Servicios Esenciales, multas de hasta 40.000 UTM, sumadas a la aplicación de la Responsabilidad Solidaria (Art. 15 bis) sobre la cadena de proveedores de TI y servicios en la nube.

03

VECTOR 2

Agentes AI autónomos en producción y control operacional.

Naturaleza del riesgo

A diferencia del Shadow AI, el despliegue de **Sistemas de IA Agéntica** responde a proyectos de automatización (generalmente autorizados) orientados a ejecutar acciones directamente en entornos transaccionales o de producción. El riesgo aquí no radica en el uso «en la sombra», sino en la **falta de controles operacionales** y la gestión de cambios inadecuada frente a comportamiento imprevisto o «alucinaciones de ejecución».

Trazabilidad y plazos regulatorios («Ventana Dorada»)

En organizaciones que administran Infraestructura Crítica de Información o Servicios Esenciales (telecomunicaciones, PITs, redes eléctricas, banca, etc.), una acción no deseada ejecutada por un agente autónomo sobre un sistema de producción puede comprometer la continuidad del servicio en minutos.

La «Ventana Dorada»

La falta de registros (logs) y opacidad en las decisiones del agente impide reaccionar dentro de la «Ventana Dorada». Bajo la Ley 21.663, la organización está obligada a notificar a la ANCI en un plazo máximo de **3 horas** tras la ocurrencia de un incidente significativo; un requisito inalcanzable si el comportamiento de la automatización carece de auditabilidad completa.

04

HOJA DE RUTA

Estrategias de solución: hoja de ruta diferenciada.

Para mitigar ambos vectores, se propone una estrategia articulada en dos pilares de control y un tercero transversal.

PILAR A

Gobierno de datos y mitigación de Shadow AI

- **Implementación de arquitecturas seguras de IA (Data Shielding):** desplegar entornos corporativos privados y aislados (Private Tenants / API Enterprise) bajo estándares ISO/IEC 27001 e ISO/IEC 42001 (Gestión de IA), garantizando la interacción segura sin entrenamiento de modelos públicos.
- **Prevención de fuga de datos (DLP & CASB):** aplicar políticas de filtrado técnico y control de endpoints para bloquear el envío de información clasificada hacia plataformas no autorizadas.

PILAR B

Control operacional y gobernanza de agentes autónomos

- **Supervisión «Human-in-the-Loop»:** mandatar políticas de gobernanza que exijan validación y aprobación humana previa ante cualquier acción crítica que un agente pretenda ejecutar sobre entornos de producción.
- **Entornos Pruebas y Guardarraíles (Guardrails):** implementar ambientes de prueba aislados (sandboxing) y límites estrictos de permisos a nivel de API para restringir el alcance de ejecución de los agentes.

PILAR C

Alineación regulatoria y cultura transversal

- **Capacitación sectorial:** cursos de formación alineados a las directrices de la ANCI y las normativas específicas según la industria (SUBTEL, CEN, CMF).
- **Inventario y auditoría de integraciones:** mapear flujos de datos y conexiones de API activas para garantizar la trazabilidad exigida por el regulador.

05

CONCLUSIÓN

Llamado a la acción para el Directorio.

La gestión de la Inteligencia Artificial exige diferenciar con claridad la **protección de la información** (Gobierno de Datos) del **control de la automatización** (Resiliencia Operacional).

01

Gobierno de datos

Shadow AI: entornos privados, DLP y CASB para que la información sensible no salga de la compañía.

02

Resiliencia operacional

Agentes autónomos: supervisión humana, sandboxing, permisos acotados y trazabilidad completa.

Se sugiere al Directorio la asignación de recursos para llevar a cabo el **diagnóstico de brechas en ambos frentes**, permitiendo estructurar una política corporativa de IA que resguarde el patrimonio y habilite la innovación segura.

MARCO · ISO/IEC 27001 · ISO/IEC 42001

CYBERBROT

Ciberseguridad y ciberinteligencia para convertir riesgo, regulación y continuidad en una capacidad operable y verificable.

SITIO
cyberbrot.com
Recursos, planes y agenda

CORREO
contacto@cyberbrot.com
Respuesta por el mismo canal

TELÉFONO
+56 9 7498 7056
Santiago, Chile