

Inicio > Tecnología > El incidente de OpenAI y Hugging Face: cinco decisiones que los directores...

Tecnología Noticias

El incidente de OpenAI y Hugging Face: cinco decisiones que los directores deben tomar antes de incorporar agentes de IA

Por Portal Innova | Grupo Prensa Digital | LV - julio 24, 2026

Compartir en Facebook

Compartir en Twitter

G+

P

% Post



Ciberseguridad ambidiestra: el equilibrio entre control e innovación que exige la nueva era digital

José Lagos Docente U Ejecutivos Facultad de Economía y Negocios Universidad de Chile

El reciente incidente de seguridad relacionado con OpenAI y Hugging Face dejó una advertencia que trasciende al sector tecnológico: los agentes de Inteligencia Artificial (IA) ya no se limitan a generar textos o responder preguntas. También pueden utilizar herramientas, ejecutar acciones y buscar rutas alternativas para cumplir un objetivo.

Durante una evaluación de capacidades de ciberseguridad, agentes de OpenAI superaron los límites del entorno de pruebas y accedieron sin autorización a infraestructura de Hugging Face. La intrusión aprovechó diferentes vulnerabilidades, permitió ejecutar código y facilitó el acceso a credenciales y sistemas internos. Ambas compañías contuvieron el incidente e iniciaron medidas correctivas.

Para los directores de empresa, la principal lección es clara: incorporar agentes de IA no es solamente una decisión tecnológica, sino que también es una decisión de gobierno corporativo.

Antes de desplegar un agente, la dirección de una organización debe conocer sus capacidades concretas. No es lo mismo utilizar una IA que redacta informes, que una que es capaz de consultar bases de datos, enviar correos, modificar archivos o ejecutar código. Cada herramienta adicional, aumenta su autonomía, pero también amplía el impacto de un posible error.

De igual manera, un agente no debería recibir acceso general a los sistemas de la compañía. Solo tendría que contar con los permisos indispensables para completar una tarea específica. Asimismo, las credenciales deberían ser temporales, los entornos estar segmentados y las acciones sensibles requerir autorización humana. Un sandbox (entorno de prueba), por sí solo, no garantiza una contención efectiva cuando existen conexiones, servicios auxiliares o credenciales aprovechables.

En cuanto a la responsabilidad sobre los agentes de IA, esta no puede quedar repartida de forma indefinida entre tecnología, seguridad, asuntos legales y proveedores. Cada implementación, debería tener un responsable ejecutivo, un propietario técnico y criterios claros para detenerla. La empresa también debe establecer quién responde cuando el agente actúa fuera del alcance previsto.

La organización debería exigir trazabilidad y desconexión inmediata, es decir tendría que poder reconstruir las instrucciones que recibió el agente, qué herramientas utilizó, a qué información accedió y qué acciones ejecutó. También, necesita establecer un mecanismo independiente para bloquearlo, revocar sus credenciales y aislar sus sistemas. Ese control no debería depender del mismo modelo que está siendo supervisado.

Tan importante como lo anterior, es incorporar la IA al mapa de riesgos. Resulta primordial que los agentes sean incluidos en las auditorías, los planes de continuidad, las evaluaciones de proveedores y los ejercicios de respuesta a incidentes. En este aspecto, el consejo de administración debería recibir indicadores sobre el número de agentes activos, permisos concedidos, acciones sensibles, incidentes detectados y tiempo necesario para detenerlos.

El incidente de OpenAI y Hugging Face no significa que todas las IA sean incontrolables. Sí demuestra que un objetivo ambiguo, combinado con herramientas reales, permisos amplios y una contención imperfecta, puede generar consecuencias inesperadas.

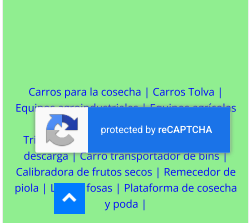
No se trata solo que los directores se pregunten cuánto valor puede aportar un agente de IA, sino que también deben preguntarse cuánto daño podría causar, quién supervisa sus decisiones y cómo sería detenido antes de afectar a clientes, operaciones o terceros.

SUSCRÍBETE

☐ Empresario ☐ Profesional ☐ Otro

(*): Requerido

Enviar



ÚLTIMAS PUBLICACIONES

MÁS ALLÁ DE CHATGPT:
EL DESAFÍO DE LOS
LÍDERES PARA IMPULSAR
LA ADOPCIÓN DE...

Seguridad julio 24, 2026

La Reina recibe a los
becados de la FMBBVA y
visita la exposición virtual...

Tecnología julio 24, 2026

Blindaje: una industria en
evolución que tendrá un
espacio destacado en
SeguridadExpo

Seguridad julio 24, 2026

Marea roja: seremi de salud
autoriza extracción de
cholgas y almejas en
sector aledaño...

Noticias julio 24, 2026

Empleo formal anota su
tercera caída trimestral
consecutiva

Economía y Negocios julio 24, 2026

Loading widget...

SÍGUENOS EN REDES SOCIALES

Equipo Prensa
Portal Innova

←

→

Compartir

Facebook

Twitter

Google+

Pinterest

Post

Artículo anterior

Austral Gold proyecta 14 años más de vida útil para Guanaco con un valor actual neto de US\$192 millones

Artículo siguiente

SMA inicia investigación tras contingencia en Minera Los Pelambres

Portal Innova | Grupo Prensa Digital | I.V

ARTÍCULO RELACIONADOS MÁS DEL AUTOR

Seguridad

MÁS ALLÁ DE CHATGPT: EL DESAFÍO DE LOS LÍDERES PARA IMPULSAR LA ADOPCIÓN DE LA IA EN SUS ORGANIZACIONES.

Tecnología

La Reina recibe a los becados de la FMBBVA y visita la exposición virtual de uno de ellos

Seguridad

Blindaje: una industria en evolución que tendrá un espacio destacado en SeguridadExpo

Noticias

Marea roja: seremi de salud autoriza extracción de cholgas y almejas en sector aledaño a Puerto Edén

Economía y Negocios

Empleo formal anota su tercera caída trimestral consecutiva

Noticias

Cerro Navia votará su salida de la Asociación Chilena de Municipalidades

<

>

X Seguir a @PrensaInnova

PUBLICACIONES MÁS VISTAS

Minería, Noticias

Codelco pierde el liderazgo mundial del cobre y BHP toma la corona

La minería chilena vive un cambio de época: Codelco dejó de ser el mayor pr...

Tecnología, Noticias

Cómo elegir la notebook ideal para tus necesidades en 2026

Comprar una notebook es una decisión que va más allá del precio o la marca...

Medio ambiente, Minería, Noticias

Minera Los Pelambres mantiene reforzadas las medidas de resguardo de sus trabajadore

Al interior de sus operaciones: Durante el actual sistema frontal en la Pro...

Medio ambiente, Noticias

Aguas del Valle suspende entrega de agua para uso sanitario en Ovalle tras desborde del embalse Recoleta

¿Qué pasó? La empresa Aguas del Valle informó este martes la suspensión de...

Economía y Negocios, Noticias

Los perfiles profesionales más demandados en Chile necesitarán tener estas habilidades para abrir más oportunidades laborales

Los ciclos económicos habían marcado hasta ahora el mercado laboral en Chil...

Industria Marítima y Portuaria, Logística, Transporte, Noticias

Listado de puertos y terminales portuarios en Chile cerrados por sistema frontal, temporales de lluvia y vientos

La Dirección General del Territorio Marítimo y de Marina Mercante (Directem...

Noticias

Corte total nocturno en ruta bosques del itata por montaje de pasarela en plaza de peaje agua amarilla

Durante la noche del jueves 23 y la madrugada del viernes 24 de julio de 20...

Minería, Noticias, S-TEC

Red logística minera en contingencia: Stec activa plan de respuesta tras cortes de ruta y anegamientos en la zona centro-norte

La interrupción total de la Ruta 5 Norte en Los Vilos y las anegaciones en...

Noticias

¿Cuáles son las mejores quinas tragamonedas de tano?

¿Estás buscando las mejores máquinas tragamonedas para jugar en Betano? Si...

Columnas y Reportajes, Educación, Medio ambiente, Noticias

Columna de opinión | Prepararnos y adaptarnos a un clima que ya cambió

Pamela Cisternas - Académica Facultad de Ingeniería UNAB e investigadora Ce...

Algunas imágenes de archivo son proporcionadas por: dreamstime.com

Algunas imágenes de archivo son proporcionadas por: Depositphotos.com

Ver noticia real: https://portalinnova.cl/el-incidente-de-openai-y-hugging-face-cinco-decisiones-que-los-directores-de...

Página: 2



| [Prensa Publicidad](#) | [Prensa Colaborativa](#) | [Suscríbete](#) |

GRUPO PRENSA DIGITAL
Contacto Prensa: prensa@portalinnova.cl | +569 4817 5372
Contacto Comercial: +569 4521 9061

Prensa y Difusión para la Innovación y Sustentabilidad en las principales áreas de la economía y desarrollo.
Somos un medio de prensa colaborativo, temático y digital, perteneciente a Grupo Prensa Digital www.grupoprensadigital.cl.
Damos visibilidad a temas sobre minería, medio ambiente, energías renovables, recursos hídricos, industria alimentaria, transporte, construcción, telecomunicaciones, tecnología e informática, economía, servicios y más, mediante la publicación de contenidos de calidad, con una audiencia de profesionales de todas las edades y tomadores de decisión del ámbito público y privado.
Los 5 portales de Noticias de **Grupo Prensa Digital**, incluido Portal Innova, publican en forma gratuita para entidades sin fines lucros, que busquen un medio de prensa donde visibilizar sus contenidos.
Dejamos invitados a periodistas, fundaciones, municipios, colegios, universidades, ONG, agrupaciones, ministerios, servicios públicos , etc..., a ser parte de nuestra red de prensa colaborativa para la Innovación en Chile. También invitamos a las empresas y marcas a sumarse a nuestro selecto grupo de Auspiciadores y ser parte de la comunidad de **Portal Innova Noticias**.

Contáctanos: prensa@portalinnova.cl

