

A blurred photograph of a modern office interior with large glass windows. Two people, a woman in a white lab coat and a man in a white lab coat, are walking across the frame from left to right. The image is overlaid with bright orange and yellow light trails, suggesting motion and technology. The overall color palette is dominated by cool blues and teals, with the light trails providing a warm contrast.

Farma y Ciberseguridad: una relación estratégica y urgente

Junio 2025

Índice

01. Resumen ejecutivo	3
02. Introducción: El ecosistema digital de la industria farmacéutica	3
03. Ciberseguridad: el pilar que protege la innovación farmacéutica	4
04. Conclusión	5
05. Referencias	6

01.

Resumen ejecutivo

La industria farmacéutica atraviesa una profunda transformación digital que, aunque genera importantes eficiencias, también expone a la organización a riesgos cibernéticos inéditos y en crecimiento. La adopción de inteligencia artificial, la integración de datos genómicos y clínicos, y la complejidad de cadenas globales de suministro hacen imprescindible incorporar la ciberseguridad como un factor estructural para proteger la propiedad intelectual, garantizar la continuidad operativa y cumplir con un marco regulatorio cada vez más exigente. Este documento analiza las principales amenazas, el entorno regulatorio y las estrategias clave para convertir la ciberseguridad en una ventaja competitiva.



02.

Introducción: El ecosistema digital de la industria farmacéutica

La industria farmacéutica es hoy uno de los sectores más digitalizados y estratégicamente expuestos. Inversiones masivas en investigación y desarrollo (I+D), el uso de inteligencia artificial para el descubrimiento de fármacos y la medicina personalizada, así como la gestión integrada de datos clínicos y genómicos, impulsan innovaciones sin precedentes. Sin embargo, esta digitalización conlleva la aparición de nuevos vectores de ataque que hace solo cinco años no existían. Forrester (2024a) proyecta que el impacto económico global del ciberdelito alcanzará los 12 billones de dólares en 2025, reflejando un riesgo creciente para cualquier empresa que no incorpore la ciberseguridad como parte central de su estrategia. La evaluación puntual de proveedores ya no es suficiente: la industria farmacéutica debe adoptar un enfoque continuo y en tiempo real para gestionar el riesgo en un ecosistema interconectado y vulnerable.

Ciberseguridad: el pilar que protege la innovación farmacéutica

Protegerse frente a riesgos cibernéticos va mucho más allá de implantar soluciones tecnológicas: implica adoptar un enfoque estratégico que refuerce la integridad de la investigación, asegure el cumplimiento normativo y garantice la resiliencia de una cadena de suministro cada vez más interconectada.

Su impacto es directo en áreas clave:

- **Investigación y Desarrollo (I+D):** Protege la propiedad intelectual y los datos experimentales, evitando pérdidas que pueden comprometer años de trabajo y millones de inversión.
- **Cumplimiento Normativo:** Responde a regulaciones cada vez más exigentes en protección de datos y ensayos clínicos, reduciendo riesgos de sanciones y daños reputacionales.
- **Cadena de Suministro:** Fortalece la seguridad operativa a lo largo de redes globales de proveedores y distribuidores, previniendo interrupciones y fraudes.
- **Reputación y Confianza:** Reafirma la credibilidad de la organización frente a pacientes, autoridades sanitarias e inversores, consolidando su posición en un mercado altamente regulado y competitivo.

Aun así, muchas organizaciones siguen viendo la ciberseguridad como un gasto operativo, en lugar de asumirla como lo que realmente es: un factor estratégico que protege su futuro.

A continuación, analizamos algunas de las amenazas actuales y emergentes que desafían a la industria farmacéutica y por qué anticiparse a ellas es clave para garantizar la continuidad de negocio y preservar la ventaja competitiva.

Conclusión

La industria farmacéutica se enfrenta a un escenario donde la ciberseguridad ya no es una opción técnica ni un gasto recuperable, sino un pilar estratégico fundamental para proteger su innovación, continuidad y reputación.

Adoptar un enfoque proactivo y estructural en ciberseguridad es la clave para seguir siendo competitivos y confiables en un entorno cada vez más digital y regulado.



05. Referencias

- Critical Medicines Alliance. (2025). Strategic Report of the Critical Medicines Alliance. https://health.ec.europa.eu/system/files/2025-02/hera_cma_strat-report_en.pdf
- Drug Discovery & Development. (2024, marzo 5). Cencora data breach exposes patient data at multiple pharma companies. <https://www.drugdiscoverytrends.com/cencora-data-breach-exposes-patient-data-pharma-firms>
- Escudo Digital. (2024, marzo 6). Violación de datos en Change Healthcare afecta a 100 millones de pacientes. <https://www.escudodigital.com>
- Forrester. (2024a). Predictions 2025: Cybersecurity, Risk, and Privacy. Forrester Research. <https://www.forrester.com/predictions>
- Forrester. (2024b). Predictions 2025: Europe Will Make A Major Statement About The AI Act. Forrester Blogs. <https://www.forrester.com/blogs/predictions-2025-europe>
- IQVIA Institute for Human Data Science. (2024). The Global Use of Medicines: Outlook to 2028. <https://www.iqvia.com/institute/reports>
- Medical Economics. (2024, marzo 4). Change Healthcare data breach affects 100 million Americans. <https://www.medicaleconomics.com/view/change-healthcare-breach-affected-100-000-000-patients>



babelgroup.com

IT CONSULTING. DIGITAL ACCELERATION. BUSINESS TRANSFORMATION.