Corporate Risk Management

INTREP: Evaluación estratégica de amenazas a la industria farmacéutica

01.07.2025

Contenido

Metodología

Objetivo

El propósito de esta evaluación estratégica de amenazas es identificar, explicar y analizar las amenazas más importantes para la industria farmacéutica en relación con sus activos. Esto proporciona un análisis de la probabilidad e impacto de las amenazas, así como una evaluación y asesoramiento general para facilitar la toma de decisiones estratégicas bien fundamentadas. El informe también destacará las vulnerabilidades comunes que afectan a las empresas del sector, incluyendo sus cadenas de suministro y valor, y que pueden ser explotadas por amenazas y exponer a las organizaciones a riesgos.

Este informe no está diseñado para una organización o ubicación geográfica específica, sino que busca describir las amenazas generales que pueden representar riesgos de seguridad, operativos y de reputación para las personas, los bienes y los activos de las empresas. Las amenazas, incluyendo su probabilidad e impacto, pueden no afectar a todas las empresas de la misma manera, por lo que se recomienda considerar el contexto específico de cada organización al leer el informe.

Niveles de amenaza

El Corporate Risk Management utiliza información recopilada tanto de inteligencia de fuentes abiertas (OSINT), como de fuentes cerradas, como la inteligencia humana (HUMINT), y se procesa y analiza antes de su evaluación y distribución final.

Niveles de amenaza

Cada sección se investiga individualmente y se califica en una escala del 1 al 5 según la probabilidad y la gravedad de la amenaza en esa ubicación específica. Posteriormente, cada sección se revisa y se incorpora a una evaluación general de la ubicación.

NIVEL EVALUADO DE AMENAZA	
5 – CRÍTICO	Amenaza muy alta/extrema. Revisar y responder si es necesario.
4 – ALTO	Amenaza alta/importante. Considere tomar las medidas adecuadas.
3 – MODERADO	Amenaza moderada. Mantenerse alerta y tomar precauciones.
2 – BAJO	Amenaza baja/limitada. Se recomienda.
1 – MUY BAJO	Amenaza muy baja/insignificante. Para concientización.

Intención y capacidad

La amenaza planteada por actores o fuentes de amenazas específicas se basa en la intención y la capacidad de llevar a cabo un curso de acción (COA).

NIVEL	INTENCIÓN	CAPACIDAD
5 - EXTREMO	El actor de amenaza está determinado en su CDA. Existe una percepción significativa de éxito o recompensa. Hay precedentes de éxito.	El actor de amenazas tiene todos los recursos necesarios para llevar a cabo su CDA, y es muy poco probable que existan limitaciones que le impidan llevarlo a cabo.

4 - ALTO	El actor de amenaza ha expresado su intención. Existe la percepción de un éxito o recompensa específica. Hay precedentes de ataques.	El actor de amenaza tiene acceso a los recursos necesarios para su CDA y, si bien existen limitaciones, es poco probable que estas lo disuadan.
3 - MODERADO	El actor de amenaza tiene una intención implícita. Existe la percepción de algún éxito. Existe un precedente limitado de éxito.	El actorde amenaza tiene cierto acceso a los recursos necesarios para su CDA, y existen algunas limitaciones que pueden disuadirlo.
2 - BAJO	El actor de amenaza no ha dado a conocer ninguna intención, aunque el objetivo es viable por su CDA. Existe una baja tasa de éxito y no hay precedentes.	El actor de amenaza tiene acceso limitado a los recursos necesarios para su CDA y existen numerosas limitaciones que probablemente lo disuadirán.
1 - MUY BAJO	El actor de amenaza no ha expresado ni hay intenciones implicitas; la recompensa es muy baja o nula y el éxito es incierto. No hay precedentes.	El actor de amenaza tiene acceso muy limitado a los recursos necesarios para su CDA y existen limitaciones significativas que muy probablemente le impedirán llevarlo a cabo.

Lenguaje de probabilidad

La evaluación de amenazas de seguridad de eventos utiliza el lenguaje de probabilidad del Corporate Risk Management para evaluar la probabilidad de que una amenaza se manifieste, basándose en la probabilidad, utilizando un porcentaje, fracción o proporción como referencia.

Esto facilita el contexto y la claridad, y ayuda a mantener un enfoque estandarizado.

LENGUAJE DE PROBABILIDAD							
TÉRMINO:	Remoto	Altamente Improbable	Improbable	Posible	Probable	Altamente probable	Casi certero
PROBABILIDAD:	0 - 4%	10 - 20%	25 - 35%	40 - 50%	55 - 75%	80% - 90%	95 - 99%

Fecha corte de inteligencia:	1600hrs UTC – 5 / 01.07.2025

Inteligencia prioritaria

NIVEL DE AMENAZA	
3 – MODERADO	Amenaza moderada. Mantenerse alerta y tomar precauciones.

AMENAZAS RELEVANTES				
Ciber ataques	*Amenazas internas*	*Clima extremo*	*Condiciones económicas*	*Cambios en la regulación*
				

- Los ciberataques representan la amenaza más importante para la industria farmacéutica, ya que los incidentes con impactos a gran escala (financieros, legales y reputacionales) ocurren con mayor frecuencia y afectan a organizaciones privadas de todo el mundo. Debido a la creciente sofisticación y complejidad de los ciberataques dirigidos a la industria, es casi seguro que seguirán siendo una amenaza clave a medio y largo plazo.

- En los últimos años, numerosos incidentes relacionados con amenazas internas han impactado cada vez más al sector farmacéutico, lo que puede provocar pérdida de datos, repercusiones financieras y legales, y daños significativos a la reputación. Es probable que los incidentes de amenazas internas, tanto maliciosas como accidentales, sigan impactando a la industria farmacéutica a medio y largo plazo, lo que indica la necesidad de implementar medidas de protección adecuadas para limitar la explotación de vulnerabilidades y los riesgos subsiguientes.

- Los fenómenos meteorológicos extremos, como tormentas, terremotos o tornados, pueden interrumpir la cadena de suministro de la industria farmacéutica, lo que afecta su operatividad y sus ganancias, además de representar amenazas para la infraestructura. Es probable que estos fenómenos se intensifiquen y se vuelvan más frecuentes junto con el cambio climático, lo que presenta un panorama de amenazas en constante evolución que impacta directamente a la industria tanto en la actualidad como a largo plazo.

- Es probable que las condiciones económicas regionales y los cambios regulatorios afecten las operaciones diarias de las organizaciones farmacéuticas, así como su rentabilidad y sus cadenas de suministro globales. La competencia en el mercado nacional y entre países probablemente sea un factor muy influyente en esta tendencia en regiones específicas, y es probable que las organizaciones modifiquen sus modelos de negocio para seguir siendo atractivas para los inversores.

El Corporate Risk Management evalúa que la industria farmacéutica tiene una alta probabilidad de verse afectada por ciberataques y amenazas internas a corto plazo, impulsadas principalmente por motivaciones financieras, tensiones geopolíticas y una mayor competitividad en el mercado. Los fenómenos meteorológicos extremos, las condiciones económicas y los cambios regulatorios también pueden afectar las operaciones de las organizaciones del sector, especialmente a través de su impacto en la cadena de valor y la consiguiente interrupción de la cadena de suministro. Es muy probable que el impacto de estos vectores de amenaza afecte las ganancias, las relaciones comerciales, el cumplimiento normativo y la

competitividad de las organizaciones, por lo que es fundamental implementar medidas de prevención y seguridad significativas para proteger a las empresas en todas las regiones.

LENGUAJE DE PROBABILIDAD							
TÉRMINO:	Remoto	Altamente Improbable	Improbable	Posible	Probable	Altamente probable	Casi certero
PROBABILIDAD:	0 - 4%	10 - 20%	25 - 35%	40 - 50%	55 - 75%	80% - 90%	95 - 99%

Antecedentes

La industria farmacéutica puede ser susceptible a diferentes vulnerabilidades y, por consiguiente, enfrentarse a múltiples amenazas, tanto accidentales como maliciosas, que pueden suponer importantes riesgos de seguridad, operativos y de reputación. Varios factores influyen en la probabilidad y el impacto potencial de amenazas específicas, como la ubicación geográfica, la accesibilidad, los controles de seguridad empleados, la legislación y las regulaciones, y los patrones climáticos.

Las amenazas accidentales a la industria farmacéutica suelen ser más difíciles de mitigar debido a su naturaleza impredecible, mientras que las amenazas maliciosas suelen seguir patrones o tendencias que pueden ayudar a definir las medidas de protección. Sin embargo, los actores asociados con estas amenazas suelen tener acceso a muchos recursos que pueden complicar los esfuerzos de mitigación o intensificar la frecuencia y el impacto de los ataques.

Debido a la sensibilidad del sector, la industria farmacéutica es un objetivo atractivo para los actores maliciosos que buscan obtener beneficios financieros, ideológicos o de notoriedad. Las acciones respaldadas por estados nacionales hostiles son una posibilidad real debido a la posible obtención de datos o propiedad intelectual que podrían utilizar en su beneficio para desarrollar sus capacidades nacionales en una industria altamente competitiva.

Activos y vulnerabilidades de la industria farmacéutica

Las amenazas a la industria farmacéutica impactan en gran medida a uno o más de los activos asociados con la industria, principalmente a través de la explotación de vulnerabilidades, de manera accidental o maliciosa, lo que plantea riesgos a las organizaciones dentro de la industria, así como a sus cadenas de suministro.

Indicadores de amenazas y riesgos específicos de la industria farmacéutica			
Amenaza	**Activo**	**Vulnerabilidad**	**Riesgo**
			
• Cambios regulatorios • Condiciones económicas • Ciberataques • Amenazas internas • Clima extremo	• Plantas físicas (fabricación, oficinas, sede central) • Investigación / Propiedad intelectual • Software (incluido software de terceros) • Redes / sistemas • Productos / servicios • Personas	• Instalaciones sin seguridad • Controles de ciberseguridad deficientes • Seguridad operativa deficiente • Cadenas de suministro sin seguridad	• Interrupción operativa • Pérdida de datos • Desabastecimiento de medicamentos • Infracciones de cumplimiento/legales • Repercusiones financieras • Desventaja competitiva • Primas de seguros

	• Cadenas de suministro • Cadena de valor		

La tabla anterior describe las amenazas, activos, vulnerabilidades y riesgos que se evalúan como prioritarios en relación con la industria farmacéutica y no incluye todos los elementos que podrían figurar en cada sección.

Amenazas que enfrenta la industria farmacéutica

Ciberataques

Los ciberataques se están convirtiendo en una amenaza cada vez más frecuente para la industria farmacéutica, impulsados en gran medida por la motivación de los cibercriminales hacia las ganancias financieras, lo que a su vez los lleva a favorecer a industrias u organizaciones, como la farmacéutica, que dependen de datos e información confidencial almacenados en sus sistemas y de su valiosa tecnología (incluida la propiedad intelectual), que puede ser extorsionada para obtener ganancias.

Los ciberataques también pueden ser implementados por cibercriminales que buscan dañar la reputación de un país u organización específica. Muchos ataques dirigidos a la industria resultan en pérdidas significativas de datos, lo que afecta directamente las relaciones con clientes, pacientes y socios comerciales. Las ciberamenazas pueden surgir de las acciones de personas internas de las organizaciones o de la industria, de forma maliciosa y accidental, lo que representa una amenaza sustancial de explotación interna, que es cada vez más difícil de mitigar para las organizaciones.

Técnicas de ciberataques

Los cibercriminales pueden implementar diversas tácticas, técnicas y procedimientos (TTP) para atacar a organizaciones, entidades y organismos gubernamentales relacionados con la industria farmacéutica. La mayoría de los ataques dirigidos a la industria se realizan para interrumpir las operaciones y obtener datos/IP, así como el pago de rescates, utilizando las TTP que se describen a continuación:

Ransomware: el ransomware es un malware diseñado para evitar que el usuario o la organización accedan a sus propios archivos cifrándolos y exigiendo el pago de un rescate por la clave de descifrado, lo que coloca a la organización en una posición en la que pagar el rescate es el método de recuperación más fácil y económico.

Ataques DoS/DDoS: La denegación de servicio (DoS) y la denegación de servicio distribuida (DDoS) son ataques maliciosos y dirigidos que interrumpen las operaciones comerciales al inundar una red con solicitudes falsas que interrumpen tareas rutinarias como acceder a correos electrónicos, sitios web u otros recursos.

Malware: software diseñado para causar interrupciones en una computadora, servidor o red y obtener acceso no autorizado a los datos.

Phishing: los actores de amenazas utilizan sitios web, correos electrónicos y mensajes de texto de apariencia legítima para atraer a las víctimas para que carguen malware que puede robar datos del dispositivo comprometido.

Ingeniería social: la ingeniería social es una técnica empleada por individuos en línea para manipular o incitar a otros a realizar acciones que podrían beneficiar al atacante o perjudicar al objetivo. Esto podría consistir en enviar información confidencial sin que lo sepa un atacante creyéndolo alguien de confianza.

Ataque Man-in-the-Middle (MitM): los ataques MitM, también conocidos como espionaje, ocurren cuando un actor de amenazas se infiltra en una transacción entre dos partes para robar o filtrar datos. Esto puede ocurrir en redes Wi-Fi inseguras, como entre los dispositivos de los visitantes y la red.

Relleno de credenciales: la inyección automatizada de datos de inicio de sesión robados para obtener acceso a cuentas proyectadas.

Los actores de ciberamenazas respaldados por estados y los hackers con motivaciones financieras, incluyendo las Amenazas Persistentes Avanzadas (APA) y las bandas de cibercriminales, son los tipos de atacantes más comunes que atacan a la industria farmacéutica. Ambos grupos poseen capacidades y recursos significativos para lograr sus objetivos. Entre los estados nacionales que suelen participar en estos ataques se incluyen principalmente China, Irán, Corea del Norte y Rusia, y se observa con mayor frecuencia que realizan ataques para obtener propiedad intelectual, como fórmulas de medicamentos, datos de investigación y datos de ensayos clínicos, para mejorar sus capacidades y perturbar los mercados. Algunos de los grupos de cibercrimen/piratería que se han observado anteriormente atacando a la industria farmacéutica incluyen: Lapsus$, Killnet, LockBit 3.0, Cl0P, BianLian y REvil.

Dado que se observa cada vez más que las organizaciones del sector colaboran con diversas organizaciones externas, incluso externas a la industria, por ejemplo, para el desarrollo de productos, las cadenas de suministro, los ensayos clínicos y la distribución, la probabilidad de impactos por ataques a la cadena de suministro ha aumentado significativamente. La industria ha trabajado cada vez más para implementar regulaciones y medidas de protección (como evaluaciones de riesgos) para reducir la probabilidad y el impacto de los ataques a la cadena de suministro. Sin embargo, estos aún ocurren, impulsados por tácticas de ataque cada vez más complejas y sofisticadas que evaden las medidas de seguridad. Esto representa una amenaza multifacética para toda la industria que puede explotar vulnerabilidades en los principales activos de esta.

Actividades significativas vinculadas a la industria farmacéutica

La siguiente tabla describe los incidentes notables que han afectado a la industria farmacéutica entre 2019 y 2024, incluidos los activos explotados.

Fecha	Activo explotado	Detalles
Agosto 2024	Redes/sistemas	McLaren Health Care fue atacado por el grupo de ransomware INC Ransom, que afectó a los hospitales del sistema de salud en Michigan, EE. UU. El ataque provocó la inaccesibilidad de las bases de datos de información de pacientes y la reprogramación de procedimientos y citas no urgentes.
Junio 2024	Redes/sistemas	Ascension, un proveedor de atención médica privado estadounidense, reveló que un ataque de ransomware a sus sistemas en mayo de 2024 la obligó a desviar ambulancias y retrasar citas. Esto se debió a que un empleado descargó accidentalmente un archivo malicioso. El ataque bloqueó el acceso a los historiales médicos electrónicos (HCE), pero, según se informa, no comprometió los datos de estos.
Febrero 2024	Redes/sistemas	Cencora confirmó que durante un ciberataque se robaron de la base de datos datos confidenciales de pacientes, además de los identificados inicialmente. El informe indica que los datos robados incluían información personal identificable e información médica protegida de pacientes de una filial.
	Redes/sistemas	Dos proveedores franceses de seguros médicos, Almerys y Viamedis, fueron blanco de ciberataques que afectaron los datos de aproximadamente 33 millones de ciudadanos franceses, incluyendo la exposición de sus números de la seguridad social y fechas de nacimiento. Se informa que los autores utilizaron ataques de phishing para obtener las credenciales de acceso a un portal utilizado por profesionales de la salud.
	Redes/sistemas	United Health Group, proveedor de servicios y pagos del sector sanitario estadounidense, fue atacado por ransomware, lo que causó graves interrupciones en farmacias, hospitales y pacientes de todo el país. United Health presuntamente pagó un rescate de 22 millones de dólares y sufrió pérdidas de 870 millones de dólares en el primer trimestre de 2024.
Diciembre 2023	Redes/sistemas	La organización alemana de atención médica Fresenius Medical Care confirmó el robo de aproximadamente 500.000 historiales de pacientes y expacientes del almacén de datos de su filial en EE. UU. La organización declaró que tuvo conocimiento del ciberincidente en septiembre, y que el hacker involucrado también reconoció públicamente haber robado datos de la organización. Fresenius Medical Care también indicó que es probable que algunos datos de sus empleados estén incluidos en la filtración.
Agosto 2023	Redes/sistemas	La farmacéutica india Granules India reportó una caída de ganancias del 62,5% en el primer trimestre de 2023. La organización atribuyó la caída a un ciberataque que afectó sus operaciones en mayo. El ciberataque fue reivindicado por el grupo de ciberdelincuencia LockBit, vinculado a Rusia, que utilizó ransomware para robar datos de Granules India, los cuales posteriormente publicó en su sitio web oscuro.
Marzo 2023	Redes/sistemas	La organización farmacéutica francesa Pierre Fabre fue atacada por un ransomware REvil y, según se informa, los piratas informáticos exigieron un rescate de 25 millones de dólares para restaurar los sistemas de TI de la organización.
Diciembre 2020	Redes/sistemas	La Agencia Europea de Medicamentos anunció que había sido objeto de un ciberataque durante el cual se accedió ilegalmente a algunos documentos relacionados con la vacuna Pfizer/BioNTech.
Noviembre 2020	Personas	Presuntos piratas informáticos norcoreanos intentaron atacar a AstraZeneca haciéndose pasar por reclutadores en LinkedIn y WhatsApp para acercarse a los empleados de la organización con ofertas de trabajo falsas, que luego implicaban el envío de documentos que supuestamente incluían descripciones de puestos de trabajo que estaban plagadas de código malicioso diseñado para obtener acceso al sistema de la víctima.
Junio 2019	Redes/sistemas	La farmacéutica suiza Roche confirmó haber sido víctima de un ciberataque que utilizó malware conocido como Winnti, presuntamente implementado por hackers vinculados al gobierno chino. La organización afirmó que el ataque no afectó a datos confidenciales.

Evaluación de la probabilidad y el impacto de las amenazas

La siguiente tabla evalúa la probabilidad y el impacto de los ataques cibernéticos en la industria farmacéutica:

Activo	Probabilidad evaluada	Impacto
Redes/sistemas	Altamente probable (80-90%)	**4 – ALTO** Es muy probable que los ciberataques dirigidos a las redes/sistemas de las organizaciones afecten significativamente sus operaciones (incluidas las cadenas de suministro). Sin embargo, un mayor enfoque en medidas robustas de ciberseguridad en toda la industria debería ayudar a reducir el impacto general. Aún se espera una interrupción operativa inmediata.
Personas	Posible (40-50%)	**4 – ALTO** La explotación de información privilegiada puede representar graves amenazas para la seguridad de la industria/organización, en gran medida debido a su capacidad para acceder a áreas potencialmente sensibles de las operaciones de una organización, siendo cada vez más difícil mitigar la presencia de información privilegiada accidental. El uso de un programa integral contra amenazas internas debería ayudar a prevenir este tipo de incidentes.
Investigación / Propiedad intelectual	Posible (40-50%)	**4 – ALTO** Los ciberataques que incluyen el robo de investigación, propiedad intelectual o datos probablemente presentarán problemas de competencia e impactarán las ventas y las relaciones comerciales de las organizaciones, lo que podría generar problemas de reputación y afectar la competitividad del mercado.
Cadenas de suministro	Posible (40-50%)	**4 – ALTO** Es muy probable que los ataques dentro de la cadena de suministro provoquen retrasos operativos, posibles problemas con el suministro de medicamentos o equipos, y pérdida de datos, lo que probablemente represente un riesgo para la reputación de las organizaciones o entidades responsables.
Software	Posible (40-50%)	**3 – MODERADO** La explotación del software de la industria/organización tiene el potencial de representar amenazas de seguridad para los datos y las operaciones de las organizaciones, cuya reparación por daños o pérdida de datos probablemente resultará costosa.

Amenazas internas

Una amenaza interna es una persona o entidad que utiliza su acceso, consciente o inconscientemente, para facilitar el acceso no autorizado a una industria/organización o a sus datos. Las amenazas internas pueden materializarse por diversos medios, como negligencia, malas intenciones y presiones externas como dificultades financieras o chantaje. Las amenazas internas negligentes o accidentales pueden surgir del desconocimiento de los protocolos o procedimientos de seguridad por parte de una persona y pueden verse agravadas por las vulnerabilidades de la organización.

Los datos disponibles públicamente sobre incidentes relacionados con amenazas internas, en particular aquellos dirigidos a organizaciones privadas, son limitados debido a los riesgos que una divulgación pública presenta para la seguridad, las operaciones, la marca y la reputación de las organizaciones afectadas. Sin embargo, los detalles de algunos incidentes recientes que han afectado a los sectores farmacéutico y

sanitario en los últimos años destacan las posibles motivaciones, tácticas e impactos de dichos incidentes, lo que puede utilizarse para garantizar la implementación de las medidas de mitigación adecuadas.

Según se informa, la mayoría de los incidentes de amenazas internas que afectan a la industria farmacéutica se deben a ataques accidentales o maliciosos contra las redes/sistemas de la industria. Las amenazas internas accidentales pueden afectar las redes/sistemas de las organizaciones industriales al provocar apagados accidentales, errores humanos que causan fallos de software o hardware o, principalmente, al implementar prácticas deficientes de ciberseguridad que permiten la explotación de ciberamenazas, como la ingeniería social y los ataques de phishing.

Los incidentes de amenazas internas maliciosas que han afectado anteriormente a las redes/sistemas de las organizaciones industriales se han relacionado principalmente con el robo de datos facilitado por los empleados, principalmente con fines económicos, pero también con fines ideológicos, de ventaja competitiva y de notoriedad, así como en respuesta a quejas en el lugar de trabajo. Las amenazas internas accidentales y maliciosas también pueden provenir de terceros, como proveedores, que pueden dañar las redes/sistemas al explotar vulnerabilidades en software, dispositivos o sistemas de terceros que pueden afectar directamente las operaciones. Ejemplos anteriores de amenazas internas ilustran cómo pueden manifestarse e impactar a las organizaciones de diversas maneras, entre ellas:

Sabotaje	Espionaje	Hurto	Violencia	Ciber
Activos físicos Actos deliberados que perturban o destruyen al personal, la propiedad o los activos físicos de una organización. (incendio provocado, vandalismo, robo, sabotaje de equipos)	**Económico** Adquisición de información económica (secretos técnicos, propiedad intelectual, etc.) para obtener beneficios estratégicos o influir en la seguridad económica de un rival. (fijación de precios, venta en corto)	**Delitos financieros** Explotación del dinero o los activos financieros de una organización con la intención de obtener un beneficio económico. (robo, manipulación del mercado, adquisiciones)	**Violencia laboral** La violencia interna incluye amenazas delictivas o destructivas que dañan la infraestructura o amenazan/dañan a personas o bienes. (disputas, ataques con armas blancas, armas de fuego, incendios provocados)	**Amenazas no intencionales** Exposición de la infraestructura de TI, los sistemas y los datos de una organización que causa daños no deseados. (prácticas deficientes de ciberseguridad, eliminación de datos o equipos sensibles de sitios web, correos electrónicos de phishing)
Virtual Uso de medios técnicos o cibernéticos para dañar o interrumpir la infraestructura virtual de una organización. (Ataques DDoS, ransomware)	**Gobierno** Actividades encubiertas de recopilación de inteligencia por parte de gobiernos o actores amenazantes vinculados a ellos para obtener una ventaja. (ciberataques, interrupción de la cadena de suministro)	**Propiedad intelectual (PI)** El robo de ideas, inventos o expresiones creativas de organizaciones para obtener una ventaja. (piratería informática, explotación de información privilegiada, accidental y maliciosa, robo de documentos o datos)	**Terrorismo** Las personas con información privilegiada pueden usar su conocimiento de la estructura, la seguridad o los sistemas de una organización para llevar a cabo ataques terroristas por una causa ideológica o política. (bombardeos, incendios provocados, ataques a empleados, amenazas QBRN)	**Amenazas intencionales** Acciones maliciosas realizadas por personas internas hostiles que utilizan medios físicos o técnicos para interrumpir o detener las operaciones de una organización. (Permitir acceso a terceros hostiles, tanto a sistemas como a dispositivos físicos, e implementar malware)

Las amenazas internas accidentales pueden surgir en el contexto de instalaciones físicas relacionadas con la industria. Acciones simples como abrir la puerta o permitir el acceso a un área con activos sensibles son

acciones comunes que podrían afectar la seguridad de las instalaciones o de la organización. Esto también puede implicar ingeniería social, donde actores externos pueden intentar engañar a personas con acceso interno para que les den acceso o revelen información que podría comprometer las instalaciones, incluyendo centros de I+D y fabricación. Las personas con acceso interno también pueden ser chantajeadas por actores externos, quienes pueden obligarlas a causar daños físicos a las instalaciones o a implementar códigos o dispositivos informáticos maliciosos para robar información o interrumpir los sistemas.

Las personas con acceso interno malintencionado también podrían intentar atacar instalaciones físicas, incluyendo sabotear la infraestructura o los sistemas internos, utilizando tácticas físicas y cibernéticas. Una queja en el lugar de trabajo puede motivarlas a apagar sistemas maliciosamente para interrumpir las operaciones o, en casos graves, provocar incendios o inundaciones que causen daños físicos a las instalaciones. También pueden intentar explotar el acceso que se les ha otorgado a sistemas o áreas sensibles o implementar dispositivos maliciosos, como memorias USB u otros dispositivos informáticos, dentro de las instalaciones para facilitar el robo de datos o la interrupción de los sistemas.

Las organizaciones competidoras pueden intentar explotar a un empleado actual o anterior de una organización rival para obtener información o propiedad intelectual con el fin de mejorar su rendimiento o para obtener beneficios económicos. Esto puede implicar ofrecerles recompensas económicas o un puesto dentro de su organización, una amenaza cada vez más común en la industria farmacéutica global. Esto puede ocurrir cuando las organizaciones competidoras ofrecen a un empleado actual o anterior de una organización rival un nuevo puesto donde se puedan explotar sus conocimientos o experiencia, o mediante la asignación de una persona específica para que trabaje en una organización rival con el fin de obtener información. Los empleados también pueden intentar robar propiedad intelectual o datos sensibles para construir su propia organización, lo que afecta a la competitividad y el rendimiento.

Es probable que las organizaciones competidoras cuenten con recursos limitados para contribuir únicamente a reclutar o pagar a personas con información privilegiada; sin embargo, su conocimiento de la industria puede darles una ventaja y mejorar sus capacidades al reclutar a personas con información privilegiada, ya que es probable que puedan presentar ofertas competitivas al intentar captar empleados de una organización rival.

Actividades significativas vinculadas a la industria farmacéutica

La siguiente tabla describe los incidentes notables que han afectado a la industria farmacéutica entre 2021 y 2024, incluido el activo explotado.

Fecha	Activo explotado	Detalles
Junio 2024	Redes/sistemas	Ascension reveló que un ataque de ransomware a sus sistemas en mayo de 2024 la obligó a desviar ambulancias y retrasar citas. Esto se debió a que un empleado descargó accidentalmente un archivo malicioso. El ataque bloqueó el acceso al historial clínico electrónico (HCE), pero, según se informa, no comprometió los datos del HCE.
Marzo 2024	Investigación / Propiedad intelectual	Johnson & Johnson demandó a un ex empleado por afirmaciones de que descargó "clandestina y maliciosamente" aproximadamente 1.000 archivos sensibles relacionados con estrategias en discos duros externos tres semanas antes de su renuncia y luego supuestamente accedió a ellos durante su empleo en la empresa rival Pfizer.
Junio 2023	Redes/sistemas	El Grupo Hospitales UL en Irlanda reveló una violación de datos en la que los datos de aproximadamente 1000 pacientes se vieron comprometidos luego de que un empleado enviara accidentalmente por correo electrónico datos confidenciales a un destinatario no identificado, incluidos los nombres de los pacientes, las fechas de nacimiento y los números de historial médico.
Noviembre 2022	Personas	AstraZeneca confirmó que un error de un usuario provocó que las credenciales de un servidor interno de AstraZeneca quedaran en el sitio de intercambio de

		código GitHub en 2021, lo que dejó datos confidenciales de pacientes expuestos durante más de un año.
Junio 2022	Redes/sistemas	Un especialista en informática fue acusado tras piratear el servidor de una organización de atención médica de Chicago donde anteriormente trabajaba como contratista, lo que afectó los exámenes y tratamientos médicos.
Marzo 2022	Personas	El NHS del Reino Unido descubrió que 130 cuentas de correo electrónico se habían visto comprometidas después de que los usuarios abrieran un correo electrónico de phishing que contenía enlaces a un inicio de sesión falso de Microsoft 365 e ingresaran sus datos de inicio de sesión.
Enero 2022	Investigación / Propiedad intelectual	En el Reino Unido, un ex científico de GlaxoSmithKline (GSK) se declaró culpable de conspirar para robar secretos comerciales de GSK para beneficiar a una organización farmacéutica china.
Noviembre 2021	Personas	Un ex empleado del Centro Médico del Sur de Georgia descargó datos privados de los sistemas informáticos del centro médico a una unidad USB el día después de renunciar y filtró las fechas de nacimiento, nombres y resultados de pruebas de pacientes con intenciones maliciosas.
	Investigación / Propiedad intelectual	Pfizer demandó a un empleado de larga data por violar su acuerdo de confidencialidad al cargar aproximadamente 12.000 archivos sin permiso a sus cuentas y dispositivos personales desde su computadora portátil proporcionada por el trabajo, antes de irse a trabajar para su competidor, en los EE. UU.
Enero 2021	Redes y sistemas	El ex vicepresidente de US Stradis Healthcare utilizó una cuenta secreta para interrumpir sus operaciones alterando 115.500 registros y borrando 2.300 del sistema informático de la organización, incluida información de envío, después de ser despedido de la organización semanas antes.
	Investigación / Propiedad intelectual	Un exdirector de inmunooncología de Merck fue acusado de un cargo de robo de secretos comerciales y un cargo de transmisión no autorizada de secretos comerciales relacionados con la producción de medicamentos de la organización aproximadamente al mismo tiempo que dejó Merck para ocupar un puesto en AstraZeneca en 2019.

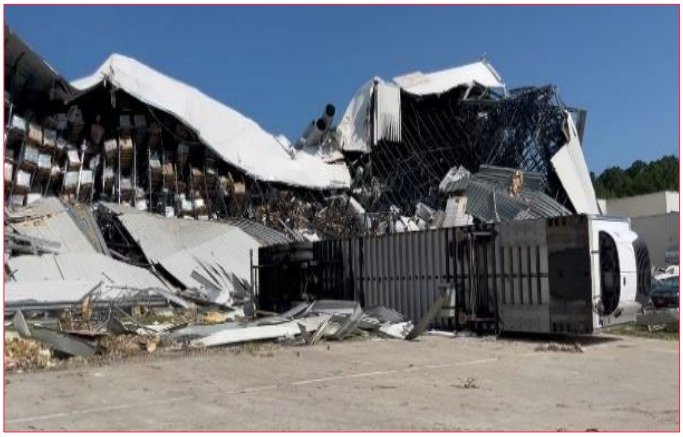
Evaluación de la probabilidad y el impacto de las amenazas

La siguiente tabla evalúa la probabilidad y el impacto de las amenazas internas en la industria farmacéutica:

Activo	Probabilidad evaluada	Impacto
Redes/sistemas	Posible (40-50%)	**4 – ALTO** Probablemente resulte en una pérdida significativa de datos, desventajas competitivas e interrupción operativa, y que también pueda afectar la reputación de la organización.
Investigación / Propiedad intelectual	Posible (40-50%)	**4 – ALTO** Probablemente resulte en una pérdida significativa de datos, desventajas competitivas e interrupción operativa, y que también pueda afectar la reputación de la organización.
Sitios físicos	Improbable (25-35%)	**4 – ALTO** Es probable que implique robo de datos, interrupción operativa y posibles daños a activos físicos. La ingeniería social tiene el potencial de provocar brechas de seguridad.
Cadenas de suministro	Improbable (25-35%)	**3 – MODERADO** Probablemente provoque interrupciones en el servicio o producto, lo que afectará la capacidad de cumplir los objetivos y, posteriormente, tendrá repercusiones financieras y un impacto en las relaciones comerciales.

Clima extremo

Incidentes de amenazas, como fenómenos meteorológicos extremos y desastres naturales, pueden causar daños accidentales a la industria farmacéutica, lo que a menudo afecta la operatividad y las cadenas de suministro, además de representar riesgos para la seguridad de los empleados. Los fenómenos meteorológicos extremos, como tormentas, deslizamientos de tierra, terremotos, incendios forestales o lluvias torrenciales, también pueden causar daños a la infraestructura, como daños a los centros de producción o instalaciones, y restringir el acceso a los centros o provocar evacuaciones.



Un tornado en la fábrica de Pfizer en Carolina del Norte causó graves daños a la infraestructura, dejándola inoperativa durante varios meses. (Fuente: X / @pfizer)

En casos extremos, los daños a la infraestructura y los activos, incluyendo los centros de producción y los equipos de fabricación, pueden causar períodos prolongados de interrupción operativa. Algunos casos recientes han tenido un impacto significativo en las ganancias trimestrales y anuales de la organización, y han provocado interrupciones sustanciales en la cadena de suministro, con retrasos en la producción y distribución de productos farmacéuticos como un impacto clave.

Los fenómenos meteorológicos extremos también pueden afectar a la industria farmacéutica mediante interrupciones en el suministro de materias primas, y eventos como sequías e inundaciones pueden afectar el crecimiento de las plantas utilizadas para producir medicamentos. Estos eventos también pueden tener una influencia significativa en la interrupción de la logística, incluyendo la aérea, terrestre y marítima, lo que puede interrumpir el acceso a materiales específicos, impactando la producción y la distribución de productos, lo que dificulta las ventas y la rentabilidad.

Es casi seguro que este tipo de amenaza varía en probabilidad e impacto según las tendencias regionales y nacionales. Las organizaciones con operaciones en ciertos países o cadenas de suministro que dependen de regiones específicas o se mueven a través de ellas, que se ven afectadas con mayor frecuencia por fenómenos meteorológicos extremos o desastres naturales, probablemente se enfrentarán a mayores riesgos.

Si bien las organizaciones farmacéuticas suelen tener un control significativo sobre sus instalaciones de fabricación, suelen tener un control y una supervisión limitados sobre las amenazas a los proveedores, incluidos los proveedores de ingredientes farmacéuticos activos (API), muchos de los cuales se encuentran en el sur y este de Asia, regiones altamente vulnerables a fenómenos meteorológicos extremos. Investigaciones previas han demostrado que incluso aumentos de temperatura leves pueden tener un impacto directo en la interrupción operativa de las plantas de fabricación, afectando la producción entre un 1 % y un 3 % debido a fallas en la maquinaria y al impacto en la mano de obra.

Latinoamérica, clave en la fabricación de productos farmacéuticos para organizaciones globales, se ha visto cada vez más afectada por fenómenos meteorológicos extremos, como huracanes y tornados, que han causado importantes daños a la infraestructura, lo que ha provocado retrasos en la producción y escasez de medicamentos. Esto ha llevado a algunas organizaciones farmacéuticas globales a retirar sus operaciones de países o regiones considerados más propensos a este tipo de amenazas. Sin embargo, es probable que esto resulte costoso y poco práctico para muchas organizaciones del sector.

Las cadenas de suministro de frío son otro elemento clave de la cadena de suministro farmacéutica, necesaria para garantizar la eficacia de ciertos medicamentos, vacunas y otros productos biofarmacéuticos.

Sin embargo, la incorporación de fenómenos meteorológicos extremos, principalmente el aumento de las temperaturas y las tormentas, presenta nuevos obstáculos que pueden dificultar la gestión del proceso. El transporte y la distribución seguros de productos farmacéuticos son un aspecto central de la cadena de suministro de la industria, con un alto potencial de que los fenómenos meteorológicos extremos o los desastres naturales que interrumpan este elemento tengan impactos en toda la industria.

El efecto de los fenómenos meteorológicos extremos y los desastres naturales en la salud mundial (el aumento de la propagación de enfermedades infecciosas y la necesidad de vacunas) también es probable que afecte a la industria farmacéutica, ya que las exigencias de las organizaciones probablemente se verán sujetas a cambios a corto plazo en respuesta a dichos eventos, lo que probablemente causará cambios operativos y consecuencias financieras. La mayoría de los fenómenos meteorológicos extremos son predecibles; sin embargo, su intensidad y frecuencia suelen cambiar y es probable que sigan teniendo un impacto cada vez mayor, lo que pone de relieve la necesidad de contar con medidas integrales de protección y resiliencia en todo momento.

Actividades significativas vinculadas a la industria farmacéutica

La siguiente tabla describe los incidentes notables que han afectado a la industria farmacéutica entre 2017 y 2024, incluidos los activos explotados.

Fecha	Activo explotado	Detalles
Junio 2024	Cadenas de suministro	Durante una de las sequías más severas en la historia reciente de México, varias partes del estado de Tamaulipas se vieron afectadas por interrupciones operativas, lo que resultó en una producción limitada o detenida, incluidas varias plantas químicas y petroquímicas.
Julio 2023	Sitios físicos	Un tornado en la fábrica de Pfizer en Rocky Mount, Carolina del Norte, causó graves daños en las instalaciones, que quedaron inoperativas durante varios meses, interrumpiendo el suministro de algunos medicamentos fabricados por la organización y causando escasez de medicamentos en todo Estados Unidos.
Agosto 2022	Sitios físicos	Las fábricas, incluidas las relacionadas con la fabricación de productos farmacéuticos, en 19 ciudades y prefecturas de la provincia de Sichuan, China, estuvieron cerradas durante seis días debido a cortes de energía durante una ola de calor.
Agosto 2020	Sitios físicos	Un incendio en una planta química en Luisiana, propiedad de BioLab, fue provocado por la aparición del huracán Laura, que golpeó directamente el lugar, provocando una fuga de cloro que luego se incendió.
Diciembre 2017	Sitios físicos	Los empleados de Amgen fueron evacuados de la sede de la organización en Thousand Oaks, California, debido a los incendios forestales cercanos, que causaron una interrupción operativa temporal.
Septiembre 2018	Sitios físicos	Según se informa, AstraZeneca se vio obligada a reducir la producción durante dos semanas en sus instalaciones de Södertälje, Suecia, debido al calor y la humedad excesivos que afectaron el proceso de fabricación.
Septiembre 2017	Cadenas de suministro	El suministro mundial de medicamentos se vio interrumpido debido al impacto del huracán María en Puerto Rico, donde contaban con aproximadamente 500 instalaciones de productos médicos. Al año siguiente, varias farmacéuticas, como Pfizer, Merck y Novartis, suspendieron la producción en sus operaciones del sureste de EE. UU. debido a la preocupación por los posibles daños o interrupciones causados por el huracán Florence.

Evaluación de la probabilidad y el impacto de las amenazas

La siguiente tabla evalúa la probabilidad y el impacto de las condiciones climáticas extremas en la industria farmacéutica:

Activo	Probabilidad evaluada	Impacto
Sitios de producción	Probable (55-75%)	**4 – ALTO** A medida que los fenómenos meteorológicos extremos se intensifican y se vuelven más frecuentes, es probable que provoquen incidentes de mayor impacto que causen interrupciones operativas y daños a la infraestructura. Si estos ocurren durante un período prolongado o en rápida sucesión, es muy probable que los costos financieros posteriores aumenten, y también es probable que aumente el impacto en la interrupción de la cadena de suministro.
Cadenas de suministro	Probable (55-75%)	**4 – ALTO** Es probable que interrumpa la fabricación y distribución de productos farmacéuticos, lo que afectará las operaciones comerciales, la rentabilidad y la reputación. Podría obligar a las empresas a reevaluar sus modelos de negocio y socios en la cadena de suministro, lo que probablemente incrementará los costos y los retrasos.
Productos/servicios	Probable (55-75%)	**3 – MODERADO** Es probable que los daños a la infraestructura o las interrupciones operativas causados por fenómenos meteorológicos extremos o desastres naturales afecten la producción de medicamentos u otros productos farmacéuticos, lo que puede afectar el suministro y causar escasez. Las medidas de resiliencia operativa deberían limitar los impactos extensos.
Redes/sistemas	Posible (40-50%)	**3 – MODERADO** Los fenómenos meteorológicos extremos o los desastres naturales pueden causar cortes de energía que afecten las redes y los sistemas de las organizaciones dentro de la industria e interrumpan las cadenas de suministro, lo que plantea desafíos operativos.
Personas	Posible (40-50%)	**3 – MODERADO** Los fenómenos meteorológicos extremos o los desastres naturales pueden representar amenazas para la seguridad de los empleados de una organización, al bloquear el acceso al lugar de trabajo o las evacuaciones, e impactar las operaciones, posiblemente durante períodos prolongados.

Condiciones económicas

Es probable que los cambios en las condiciones económicas, tanto a nivel nacional como regional y global, afecten directamente a las organizaciones de la industria farmacéutica, obstaculizando sus operaciones, rentabilidad y oportunidades de inversión. Algunas tendencias económicas pueden ser específicas de cada país o región; sin embargo, su potencial impacto global se debe probablemente a las extensas cadenas de suministro de la industria.

Los principales tipos de tendencias económicas que pueden afectar las operaciones de las organizaciones, y sus aspectos específicos, incluyen:

Inflación	Tasas de interés	Tipos de cambio
Costos de las materias primas: el aumento de los costos causado por la inflación probablemente afecte los costos generales de una organización,	**Inversiones:** Es probable que la tasa de interés actual influya en la decisión de las organizaciones con respecto a posibles oportunidades de inversión, y	**Mercados emergentes:** Las fluctuaciones del tipo de cambio pueden tener un impacto significativo en las organizaciones farmacéuticas

lo que hará que estos afecten los precios de los productos y servicios, y probablemente generen una reacción negativa de los consumidores.	cuando las tasas de interés son altas, es probable que esto impida que algunas organizaciones aprovechen dichas oportunidades, lo que probablemente afecte las operaciones y la rentabilidad.	que operan en mercados emergentes, y las diferencias en los tipos de cambio probablemente generen costos operativos variables (importación/exportación, mano de obra).
Costos laborales: Se observa que los costos laborales han seguido aumentando en los últimos años, incluso dentro de las propias organizaciones farmacéuticas y en la cadena de suministro.	**Mercados de valores:** Las tasas de interés variables influyen en el desempeño de los mercados de valores, lo que se correlaciona con el desempeño financiero de las organizaciones y posteriormente impacta en la confianza de los inversores.	**Fusiones y adquisiciones:** Los tipos de cambio pueden influir en la valoración de las organizaciones, lo que a su vez puede afectar las fusiones y adquisiciones. Cuando los tipos de cambio son altos, algunas empresas pueden verse imposibilitadas de completar las fusiones o adquisiciones deseadas, lo que afecta sus operaciones. Durante períodos de tipos de cambio bajos, puede resultar financieramente inapropiado para las organizaciones que deseen vender su negocio (o parte de él), lo que puede causarles dificultades financieras, especialmente en períodos de dificultades económicas.
Costos de I+D: Los costos de desarrollo de nuevos medicamentos, incluido el uso de tecnologías emergentes, los ensayos y el cumplimiento de las regulaciones, han seguido aumentando, a veces por encima de la tasa de inflación.	**Costos de financiamiento:** Los cambios en las tasas de interés pueden afectar los costos asociados con la obtención de financiamiento para las organizaciones, lo que puede afectar sus estrategias de precios, así como su capacidad para emprender proyectos específicos, lo que puede retrasar la expansión o disuadir a los inversores.	
Costos regulatorios: Las regulaciones que las organizaciones deben cumplir son cada vez más complejas y requieren tiempo para implementarlas y garantizar su cumplimiento, lo que les genera costos a lo largo del proceso. Los costos asociados con el incumplimiento también han aumentado.		

Algunas tendencias recientes relacionadas con las condiciones económicas han impactado directamente a la industria y a las organizaciones dentro de ella, y se espera que algunas continúen expandiéndose e influyendo en la industria en el largo plazo, presentando diversas amenazas que es muy probable que deban mitigarse para garantizar que las operaciones puedan continuar.

Emergencias sanitarias globales	Preocupaciones sobre los precios de los medicamentos	Competencia en el mercado
La pandemia de COVID-19 puso de manifiesto las vulnerabilidades de la industria, con retrasos, recortes de financiación y cambios presupuestarios que afectaron las ventas y el desarrollo de fármacos, lo que sigue impactando al sector.	Las organizaciones y los reguladores de la industria se han visto sometidos a una presión cada vez mayor para reducir los precios de los medicamentos a fin de mejorar la accesibilidad y reducir la desigualdad.	El mercado farmacéutico es cada vez más competitivo en cuanto al desarrollo de medicamentos, estrategias de precios y oportunidades de inversión.
Las emergencias sanitarias mundiales también pueden obligar a las organizaciones a modificar sus prioridades de I+D y fabricación con poca antelación para satisfacer la demanda, lo que puede tener repercusiones financieras.	Es muy probable que siga siendo una política clave para los gobiernos a nivel mundial en el plazo inmediato, lo que significa que las organizaciones tendrán que cambiar sus estrategias operativas, modelos de precios y enfoques de inversión, así como potencialmente introducir medidas de ahorro de costos, como reducciones de personal.	Esto se ha intensificado aún más debido a la introducción de otros "grandes actores" en el mercado, en gran medida relacionados con los minoristas, como Amazon, lo que ha cambiado la forma en que opera la industria en cuanto a la difusión de productos, con algunas organizaciones incapaces de mantenerse al día con las demandas cambiantes.

Actividades significativas vinculadas a la industria farmacéutica

La siguiente tabla describe los incidentes notables que han afectado a la industria farmacéutica entre 2018 y 2024, incluidos los activos explotados.

Fecha	Activo explotado	Detalles
Mayo 2024	Productos/servicios	Estados Unidos aumentó los aranceles a los productos médicos importados de China, incluidos los aranceles a las jeringas y agujas, que aumentaron del 0% al 50%, y a los respiradores y mascarillas faciales, que aumentaron del 0% al 7,5% al 25%, como parte de los esfuerzos para impulsar la producción nacional.
Septiembre 2022	N/A	A medida que las tasas de interés aumentaron en septiembre de 2022, el número de fusiones y adquisiciones en la industria farmacéutica aumentó un 2,4%~ (seis~ acuerdos por mes), frente al 1,4%~ observado en promedio entre 2018-19.
Febrero 2021	Productos/servicios	La pandemia de COVID-19 provocó un aumento en la demanda de productos médicos, incluyendo EPI, equipos médicos y productos farmacéuticos. Algunos países impusieron restricciones a la exportación, lo que causó interrupciones en las cadenas de suministro. Según la Organización Mundial del Comercio, 85 países impusieron dichas restricciones, y el 58% de los productos afectados eran dispositivos médicos o consumibles médicos.
Febrero 2018	Productos/servicios	Se observó que el bajo desempeño de la lira turca impactó directamente las finanzas de las organizaciones farmacéuticas del país, incluso a través del aumento de los costos para las organizaciones que importan materias primas y otros productos al país.

Evaluación de la probabilidad y el impacto de las amenazas

La siguiente tabla evalúa la probabilidad y el impacto de las condiciones económicas en la industria farmacéutica:

Activo	Probabilidad evaluada	Impacto
Productos/servicios	Probable (55-75%)	**3 – MODERADO** Es probable que los cambios en las tasas de interés y la inflación influyan en los costos de una organización (materias primas, fabricación, mano de obra), lo que repercute en la rentabilidad y la confianza de los inversores.
Cadenas de suministro	Probable (55-75%)	**3 – MODERADO** Es probable que las tasas de interés o los tipos de cambio elevados afecten los costos de los materiales y los aranceles de exportación e importación, lo que repercutirá en los gastos generales de las organizaciones y probablemente cause interrupciones en la cadena de suministro.
Fusiones/adquisiciones	Posible (40-50%)	**3 – MODERADO** Las condiciones económicas cambiantes pueden afectar la valoración de las organizaciones, influyendo en los costos asociados a las fusiones y adquisiciones, lo que puede causar retrasos en las expansiones de las organizaciones e influir en sus ventas y estrategias.

Cambios en la regulación

La industria farmacéutica opera en un entorno altamente regulado, con numerosos organismos reguladores a nivel mundial centrados en el cumplimiento de las regulaciones en constante evolución, principalmente en materia de seguridad y eficiencia. Las condiciones políticas nacionales, incluyendo las políticas y la

legislación, pueden afectar directamente a la industria farmacéutica y a las organizaciones que la conforman, causando interrupciones operativas e influyendo en su funcionamiento.

Las organizaciones deben garantizar el cumplimiento normativo para evitar repercusiones legales y financieras, así como daños a la reputación, en línea con las preocupaciones ambientales, sociales y de gobernanza (ESG). El incumplimiento de las regulaciones puede resultar en multas, demandas e incluso encarcelamiento.

Las operaciones de las organizaciones farmacéuticas están sujetas a controles en casi todos los niveles, incluyendo I+D, fabricación, distribución/ventas y marketing, lo que resalta la importancia de la monitorización continua y la adaptación a los cambios en los requisitos regulatorios en todas las etapas. Las regulaciones y la legislación son dos tipos de controles que pueden afectar a la industria, como se describe a continuación.

- **Legislación:** la legislación se refiere a la creación de leyes que generalmente son escritas por las autoridades para satisfacer necesidades presentes y futuras, en gran medida a través de la creación de regulaciones basadas en la ley.

- **Reglamentos**: los reglamentos son reglas establecidas por una agencia/organismo rector que interpreta las leyes para facilitar su implementación.

Para cumplir con la legislación y las regulaciones, las organizaciones a menudo deben modificar sus prácticas operativas, incluyendo cambios en las especificaciones de los productos, el abastecimiento, el uso de la tecnología, el uso/almacenamiento de datos y las técnicas de marketing. Esto también puede variar significativamente según el país/región, las condiciones económicas, las tensiones geopolíticas y otras condiciones cambiantes que pueden afectar el panorama regulatorio.

Algunas de las principales áreas de preocupación en el cumplimiento normativo para la industria son los impactos ambientales, el abastecimiento ético y el uso de la tecnología, principalmente la inteligencia artificial (IA), que probablemente seguirán siendo cuestiones centrales para las operaciones comerciales a medio y largo plazo.

Junto con esto, existe un enfoque creciente en la transparencia y la protección de datos, derivado también del impacto de otras amenazas en la industria, como los ciberataques y las amenazas internas, lo que pone de relieve la influencia mutua de estos factores.

Las organizaciones se ven cada vez más obligadas a invertir grandes cantidades para garantizar su cumplimiento, incluyendo la adopción de nuevos sistemas/tecnologías que faciliten el proceso, lo que puede agilizar las operaciones, pero también suponer una carga financiera adicional. Sin embargo, la mayoría de las leyes y regulaciones impuestas a la industria están sujetas a diversos periodos de consulta que incluyen la participación de organizaciones y organismos reguladores, con el fin de garantizar que su implementación no tenga impactos negativos.

Es improbable que se impongan cambios significativos en la legislación o las regulaciones con poca antelación, lo que significa que las organizaciones suelen tener tiempo para prepararse para su implementación, lo que limita los impactos significativos. Sin embargo, esto puede ocurrir en respuesta a circunstancias imprevistas específicas, como emergencias sanitarias mundiales, lo que indica que las organizaciones deben asegurar que sus medidas de resiliencia y respuesta estén listas para implementarse en todo momento.

Evaluación de la probabilidad y el impacto de las amenazas

La siguiente tabla evalúa la probabilidad y el impacto de los cambios regulatorios en la industria farmacéutica:

Activo	Probabilidad evaluada	Impacto
Cadenas de suministro	Probable (55-75%)	**4 – ALTO** Los cambios en las regulaciones comerciales e importadoras pueden obstaculizar significativamente las operaciones comerciales y se han implementado cada vez más como resultado de las tensiones geopolíticas, que se prevé persistirán a medio y largo plazo. Esto podría obligar a algunas empresas a reubicar algunas funciones o activos, lo que probablemente impondrá costos sustanciales.
Investigación / Propiedad intelectual	Posible (40-50%)	**3 – MODERADO** Los cambios en las regulaciones relacionadas con la ética, el impacto ambiental y el uso de la tecnología probablemente obstaculicen la capacidad de una organización para llevar a cabo algunos proyectos de investigación, lo que impacta el desarrollo de productos y la rentabilidad.
Sitios físicos	Posible (40-50%)	**3 – MODERADO** Es probable que los cambios legislativos tengan impactos operativos. Sin embargo, dado que es improbable que se implementen con poca antelación, esto debería permitir a las organizaciones reaccionar eficazmente y limitar las interrupciones generales. Se deben considerar los impactos en la competitividad y la rentabilidad.

Evaluación de Inteligencia

Principales amenazas a la industria farmacéutica (ataques cibernéticos, amenazas internas, condiciones climáticas extremas, condiciones económicas, cambios regulatorios)				
Tipo de amenaza:	**Seguridad**	**Operaciones**	**Marca y reputación**	**Nivel de Amenaza**
Impacto:	**4 – ALTO**	**3 – MODERADO**	**3 – MODERADO**	**3 – MODERADO**

El Corporate Risk Management considera que la industria farmacéutica tiene mayor probabilidad de verse afectada por ciberataques y amenazas internas a corto plazo, impulsados principalmente por motivaciones financieras, tensiones geopolíticas y una creciente competitividad en el mercado. Los fenómenos meteorológicos extremos, las condiciones económicas y los cambios regulatorios también podrían afectar las operaciones de las organizaciones del sector, especialmente a través de su impacto en la cadena de valor y la consiguiente interrupción de la cadena de suministro. Es muy probable que la influencia de estos vectores de amenaza afecte las ganancias, las relaciones comerciales, el cumplimiento normativo y la competitividad de las organizaciones, por lo que es fundamental implementar medidas de protección significativas para proteger a las empresas en todas las regiones.

Los ciberataques representan la amenaza más importante para la industria farmacéutica y están aumentando en sofisticación y complejidad, lo que probablemente seguirá representando amenazas operativas, de seguridad, financieras, legales y de reputación para un mayor número de organizaciones farmacéuticas a medio y largo plazo.

- Los incidentes de ciberamenazas con impactos a gran escala (financieros, legales y reputacionales) ocurren con mayor frecuencia y afectan a organizaciones farmacéuticas privadas de todo el mundo, lo que pone de relieve la magnitud de la amenaza y su potencial para afectar directamente a las organizaciones, así como a las cadenas de suministro.

- Los ataques en cualquier etapa de la cadena de suministro pueden afectar las operaciones de la organización, incluyendo investigación y desarrollo, producción, difusión y relaciones comerciales/con inversores, lo que puede tener importantes repercusiones financieras, como el impacto en las primas de seguros y los contratos con proveedores/clientes, así como posibles problemas de cumplimiento legal y normativo.

- Las organizaciones farmacéuticas que han sido objeto de ciberamenazas a gran escala y de alto perfil en los últimos años han sufrido importantes daños reputacionales, lo que ha afectado a su rendimiento financiero trimestral y anual, y, en el peor de los casos, podría obligar a las empresas a cesar sus operaciones. • Certificar que una organización cuenta con controles adecuados para prevenir un ataque cibernético es imperativo para todas las empresas, y es cada vez más importante que las organizaciones se aseguren de tener implementados procesos de recuperación adecuados, como pólizas de seguro, ya que la probabilidad de que las organizaciones privadas se vean afectadas directa o indirectamente por incidentes de amenazas cibernéticas continúa aumentando.

Es probable que los incidentes de amenazas internas, tanto maliciosas como accidentales, sigan afectando a la industria farmacéutica en el mediano a largo plazo por parte de actores respaldados por el Estado y de la competencia, incluida la pérdida de datos, repercusiones financieras y legales y daños significativos a la reputación, lo que requiere que las organizaciones empleen medidas de protección y prevención adecuadas para limitar la explotación de vulnerabilidades y los riesgos posteriores.

- Es cada vez más probable que los empleados maliciosos se vean influenciados por el lucro, ya que a menudo poseen la capacidad de robar y vender datos, propiedad intelectual, información confidencial o secretos comerciales, y de robar dinero utilizando su acceso legítimo y autorizado al personal, la propiedad o los activos de una organización a agentes estatales hostiles, otras organizaciones o bandas criminales para obtener ganancias económicas.

- Incidentes recientes de amenazas internas en la industria farmacéutica han indicado una tendencia generalizada entre los empleados de la organización que aprovechan su acceso a los sistemas para robar datos antes, o en algunos casos después, de trasladarse a otra organización. Las organizaciones competidoras pueden intentar explotar a un empleado actual o anterior de una organización rival para intentar obtener información o propiedad intelectual con el fin de mejorar su rendimiento o para obtener ganancias económicas. Esto puede implicar ofrecerles recompensas en efectivo o un puesto dentro de su organización.

- Es probable que las organizaciones competidoras cuenten con recursos limitados para contribuir únicamente al reclutamiento o pago de amenazas internas; sin embargo, su conocimiento de la industria puede darles una ventaja y mejorar sus capacidades al intentar reclutar personal interno, ya que es probable que puedan presentar ofertas competitivas al intentar captar empleados de una organización rival.

Es muy probable que los fenómenos climáticos extremos y los desastres naturales sigan representando una amenaza importante para la industria farmacéutica, en gran medida debido al daño que pueden causar a la infraestructura y la influencia que tienen en la interrupción de la cadena de suministro, y es probable que el cambio climático siga impulsando un aumento en la frecuencia e intensidad de dichos eventos a largo plazo.

Es muy probable que garantizar que todas las plantas cuenten con las medidas adecuadas de protección contra fenómenos meteorológicos extremos y desastres naturales tenga una influencia considerable en el nivel de daños o interrupciones causadas. Se deben considerar planes de respuesta ambiental específicos para cada escenario, como los diferentes peligros ambientales, incluyendo fenómenos meteorológicos

extremos, y planes para diversificar las cadenas de suministro, para garantizar la resiliencia operativa a largo plazo.

- La interrupción operativa causada por estos fenómenos puede tener un impacto a largo plazo, especialmente en casos donde se producen daños significativos en la infraestructura, además de representar amenazas para la seguridad de los empleados. Las grandes inundaciones, tormentas eléctricas u olas de calor pueden interrumpir las redes de transporte y presentar amenazas más significativas para los activos (es decir, las redes o ubicaciones de almacenamiento refrigerado) y el bienestar de los empleados.

- Por ejemplo, la exposición prolongada a períodos prolongados de calor extremo puede afectar la producción de una planta al reducir su capacidad para mantener la capacidad de refrigeración durante las olas de calor. Si bien estos tipos de peligros pueden no representar amenazas inmediatas, los impactos operativos y comerciales son consecuencias realistas a medio y largo plazo si las organizaciones farmacéuticas no toman las medidas adecuadas, como garantizar que los sistemas de refrigeración tengan la capacidad suficiente y sean energéticamente eficientes.

- Si bien la industria farmacéutica no puede eliminar todos los riesgos a la producción, al implementar las mejores prácticas de la industria y colaborar con las agencias gubernamentales, las organizaciones farmacéuticas pueden prepararse adecuadamente para la amenaza persistente y creciente del clima extremo.

Es probable que las cambiantes condiciones económicas sigan afectando las operaciones de la industria y las organizaciones dentro de ella, incluida su capacidad para avanzar en la investigación, asegurar expansiones comerciales y atraer inversores, lo que influirá en su capacidad para ser fuertes contendientes en un entorno de mercado global cada vez más fuerte.

- Es probable que la alta demanda de productos/servicios de la industria favorezca la expansión y el desarrollo continuos de las organizaciones que la conforman. Sin embargo, es probable que la creciente preocupación por los precios de los medicamentos y las negociaciones posteriores se intensifique a medida que persistan estas demandas.

- Esto también podría variar según la ubicación de la organización, su área de operaciones y su cadena de suministro, lo que indica que las organizaciones globales probablemente se enfrentarán a numerosos cambios que deberán considerarse como parte de sus operaciones generales.

- A medida que las condiciones económicas globales continúan empeorando y los mercados se vuelven más competitivos, es probable que aumente la posibilidad de que las organizaciones competidoras implementen o exploten amenazas internas.

- Otras condiciones globales, como sanciones, tensiones geopolíticas y conflictos, también podrían influir en las condiciones económicas, lo que puede afectar las operaciones de las organizaciones farmacéuticas, las cuales pueden cambiar con poca antelación, complicando e intensificando la amenaza.

Es probable que los cambios en la regulación y la legislación sigan influyendo en las operaciones de las organizaciones de la industria, incluida una mayor presión sobre las organizaciones en torno a sus compromisos ESG.

- Más allá de las posibles repercusiones legales y financieras del incumplimiento, es muy probable que las preocupaciones relacionadas con los aspectos ESG perjudiquen la reputación de las organizaciones, lo

que probablemente se materialice en reacciones negativas de los clientes, impactos negativos en la confianza de los inversores, boicots y, en algunos casos, ataques de activistas.

- Es probable que la implementación de nuevas leyes y regulaciones en el sector se someta a diversos procesos de consulta y no se implemente sin conocimiento previo, lo que permitirá a las organizaciones adaptar sus procesos y políticas para limitar las interrupciones significativas. Sin embargo, es probable que se produzcan impactos a largo plazo en sus operaciones generales.

- Es probable que se produzcan cambios a corto plazo en las regulaciones y legislaciones en respuesta a situaciones críticas, como emergencias sanitarias, pandemias y prioridades de medicación (por ejemplo, vacunas), que pueden tener un impacto inmediato en las operaciones, lo que pone de relieve la necesidad de que las organizaciones se aseguren de ser resilientes y capaces de adaptarse a las demandas del cambio con efectos casi inmediatos.

Recomendaciones

Para facilitar la toma de decisiones dinámica ante una posible amenaza a la industria farmacéutica, o en preparación para ella, se presenta a continuación una lista de opciones tácticas (es decir, acciones de planificación a nivel gerencial) y opciones operativas (es decir, operaciones de seguridad) para consideraciones estratégicas y de seguridad. Esta lista no es exhaustiva, y las organizaciones deben considerar los controles y acciones específicos de la organización y del centro, relevantes para su operación específica.

Medidas generales de seguridad operativa y resiliencia

- Desarrollar e implementar un plan integral de respuesta a incidentes (PRI). Este describe quién debe hacer qué al responder a un incidente detectado para minimizar los daños, lo que ayuda a proteger la reputación de la empresa y las relaciones con clientes y socios. Asegúrese de que el PRI se revise periódicamente y, cuando corresponda, se pruebe mediante simulacros y ejercicios prácticos.

- Asegúrese de que todos los empleados, no solo los oficiales de seguridad, conozcan la amenaza, las tácticas y el impacto potencial del reconocimiento hostil, y de que existan procedimientos internos claros de informes y respuesta. Revise la estrategia de patrullaje (sea impredecible) y mejore la monitorización de CCTV para centrarse en áreas, entradas y puntos de vista vulnerables. Asegúrese de que el CCTV sea adecuado para la tarea para la que se utiliza.

- Clasifique la información dentro de su organización según su sensibilidad y el impacto potencial de ser comprometida por un agente de amenazas, y desarrolle y mantenga controles de información para limitar el acceso únicamente a los empleados esenciales. Asegúrese de que existan controles claros y proporcionados para detallar las prácticas de intercambio de información, y de que todos los aspectos de la empresa sean conscientes de sus responsabilidades para proteger la CII. • Revise los planes de seguridad y resiliencia, incluyendo planes de continuidad de negocio, gestión de crisis y comunicación de crisis, así como planes específicos para cada escenario.

- Garantice el cumplimiento normativo, incluyendo la consideración de la legislación regional o nacional.

- Evalúe su exposición indirecta y directa a la amenaza específica, en el contexto de su organización (es decir, ¿su organización está vinculada a un conflicto o a una demanda terrorista debido a sus

operaciones, cadena de suministro o iniciativas ESG?, y evalúe específicamente la amenaza para su personal, incluyendo a las personas importantes (VIP), basándose en el terreno humano).

- Se recomienda encarecidamente a las organizaciones desarrollar e implementar programas eficaces de identificación y detección de amenazas internas, que incluyan un enfoque en indicadores de comportamiento/rasgos explotables, violaciones de seguridad reiteradas e intentos innecesarios de involucrarse en áreas sensibles o restringidas, combinando recursos humanos y tecnología.

- Realice una evaluación de los actores de amenazas más probables para su sector y organización: organizaciones rivales, actores estatales hostiles, empleados insatisfechos, etc. Cada actor de amenazas tendrá diferentes motivaciones y podría utilizar TTP específicas. Identificar posibles amenazas puede ayudar a detectar vulnerabilidades en los procedimientos de seguridad. Las organizaciones deben mantener un conocimiento situacional para identificar de forma preventiva problemas o tendencias que puedan provocar un aumento de las amenazas internas, ya sea dirigidas específicamente a la organización, a sus socios o a las cadenas de suministro.

- Eduque al personal sobre los posibles riesgos y las fuentes de espionaje, incluyendo los peligros de la ingeniería social. Establezca procesos claros y detallados para reportar inquietudes o comportamientos sospechosos, incluyendo casos de contacto sospechoso en redes sociales y correos electrónicos.

- Las organizaciones deben realizar una investigación adecuada de antecedentes de posibles empleados y contratistas, así como establecer y mantener un programa eficaz contra amenazas internas.

Medidas específicas de la industria farmacéutica

- Realizar inspecciones y pruebas periódicas de los equipos e infraestructura de red para identificar posibles problemas.

- Realizar evaluaciones de riesgos en las cadenas de suministro, incluyendo posibles interrupciones, y tener en cuenta los posibles incidentes que puedan surgir sin previo aviso y afectar a las cadenas de suministro (clima extremo, conflictos, emergencias sanitarias mundiales). Contar con cadenas de suministro diversificadas es fundamental.

- Asegurarse de que el software de los dispositivos y equipos se mantenga actualizado para mitigar la posible explotación de vulnerabilidades.

- Implementar planes de respuesta empresarial y designar un equipo de respuesta a incidentes para desplegarse en caso de interrupción (incluyendo la cadena de suministro, las comunicaciones internas y externas).

- Realizar inspecciones y mantenimiento frecuentes de los activos de infraestructura (instalaciones de I+D, plantas de fabricación, infraestructura logística) para identificar y mitigar vulnerabilidades.

- Utilizar protocolos de seguridad operativa (OPSEC) sólidos en las ubicaciones de infraestructura crítica sensible, incluyendo el intercambio de información en línea y verbal.

- Mantenerse al tanto de las tendencias delictivas locales, incluyendo robos, que pueden tener como objetivo infraestructura crítica, incluso en la industria farmacéutica. • Mantenerse al tanto de las

actividades de protesta dirigidas a (o en las inmediaciones de) las instalaciones farmacéuticas e implementar controles de seguridad física adicionales (agentes de seguridad, patrullas móviles, CCTV) para limitar posibles daños o interrupciones.

- Instalar sistemas de detección y extinción de incendios para proteger los equipos y la infraestructura de daños por incendio.
- Implementar medidas de mitigación de inundaciones, como sistemas de drenaje y sistemas de inundación elevados, para limitar los daños.
- Mantenerse al tanto de las tendencias delictivas locales, incluidos los robos, que pueden tener como objetivo las instalaciones farmacéuticas.
- Instalar sistemas UPS (se recomiendan varios según el tamaño y la capacidad de la instalación) para proporcionar energía de respaldo inmediata en caso de cortes o fallas eléctricas.