Evaluación y Análisis de Riesgos de la Información en SpaceX: Un Estudio Basado en el Marco ISO 27001

Santiago Potes

24/8/25

1. Resumen Ejecutivo

El presente informe constituye un análisis detallado de la postura de seguridad de la información en SpaceX, una organización de carácter estratégico y relevancia geopolítica. Se ha llevado a cabo una evaluación rigurosa de los riesgos asociados a cuatro activos de información de alta criticidad: los planos de cohetes y diseños de propulsión, la investigación y los modelos de inteligencia artificial (IA), las credenciales de sistemas y agentes de IA, y los datos personales de los empleados. La metodología aplicada se alinea con los principios de la norma ISO 27001, utilizando una matriz de riesgos para identificar, analizar y proponer controles de mitigación.

Los hallazgos principales de este análisis trascienden las vulnerabilidades técnicas, destacando la importancia crítica de los factores humanos y organizacionales. Se ha identificado que la interconexión entre los servicios comerciales y los contratos de defensa, la cultura corporativa interna y la gestión del talento son vectores de riesgo tan significativos como las amenazas cibernéticas externas. El ciberespionaje patrocinado por estados, la manipulación de datos de entrenamiento de IA con consecuencias catastróficas y el riesgo inherente a una cultura laboral hostil son solo algunos de los riesgos que demandan una atención inmediata. Como resultado de este estudio, se propone una estrategia de mitigación integral que va más allá de los controles técnicos, priorizando la gestión del riesgo interno y la protección rigurosa de la cadena de suministro de IA y las credenciales de acceso.

2. Contexto de la Organización (Marco de Referencia)

2.1 Descripción de SpaceX

SpaceX, fundada con la creencia fundamental de que un futuro multiplanetario es más emocionante que uno que no lo es, opera bajo la misión de "revolucionar la tecnología espacial, con el objetivo final de permitir que las personas vivan en otros planetas".[1] Esta misión no es meramente corporativa, sino que posiciona a la compañía en el epicentro del avance tecnológico y la exploración humana, elevando el valor de su propiedad intelectual a un nivel estratégico y geopolítico. Su visión a largo plazo es "hacer que la vida sea multiplanetaria estableciendo una ciudad autosostenible en Marte".[1]

La empresa ofrece un conjunto de productos y servicios que la sitúan como líder en la industria aeroespacial. Su línea de negocio principal incluye el desarrollo y operación de la nave espacial totalmente reutilizable Starship y el cohete Super Heavy, diseñados para transportar tripulación y carga a la órbita terrestre, la Luna, Marte y más allá.[2] Además, SpaceX es el proveedor de servicios de lanzamiento líder a nivel mundial, utilizando sus cohetes Falcon 9 y Falcon Heavy, conocidos por su fiabilidad y reutilización, para clientes comerciales y gubernamentales.[2] Otro servicio fundamental es Starlink, una avanzada constelación de satélites en órbita baja que proporciona internet de banda ancha de alta velocidad a nivel global.[2] Su servicio Starshield, diseñado para uso de defensa nacional en Estados Unidos, destaca la interconexión crítica entre sus operaciones comerciales y gubernamentales, una relación que conlleva implicaciones de seguridad nacional.[3]

El entorno en el que opera SpaceX está sujeto a una regulación estricta, con entidades como la NASA que emiten directrices de ciberseguridad para el desarrollo de naves espaciales, aunque estas guías no siempre son de carácter obligatorio.[4] La empresa compite en un sector altamente dinámico y con múltiples actores a nivel global.[5]

2.2 Análisis del Entorno Estratégico

El análisis del entorno estratégico de SpaceX revela una serie de factores tanto externos como internos que influyen directamente en su postura de seguridad. En el ámbito externo, la empresa opera en un sector que ha experimentado un aumento alarmante en los

ciberataques, con la industria de la aviación registrando un incremento del 600% en el último año.[6] La mayoría de estos incidentes se centran en el robo de credenciales y el acceso no autorizado a sistemas críticos.[6] El ciberespionaje dirigido a la industria aeroespacial es una amenaza persistente y bien documentada, con actores patrocinados por estados y elementos criminales buscando robar ideas y diseños.[7] Esta situación se agrava por la naturaleza de doble uso de la tecnología de SpaceX, que atiende tanto al mercado comercial como a socios de defensa de EE. UU. como el Departamento de Defensa (DOD).[3] Esta dualidad hace que la empresa sea un objetivo primordial no solo para el espionaje corporativo, sino también para el espionaje a nivel de estado.

A nivel interno, SpaceX cuenta con una infraestructura tecnológica significativa, incluyendo centros de datos propios que requieren una administración y gestión de hardware y sistemas, como servidores y equipos de red.[9] Sin embargo, se han reportado preocupaciones sobre el factor humano y la cultura organizacional. Documentos de la matriz de riesgos señalan la importancia de la "capacidad del personal" y la "seguridad" como factores internos clave.[5] No obstante, denuncias de empleados y extrabajadores han puesto de manifiesto un ambiente laboral hostil, con problemas de "gestión caótica," "líderes tóxicos," y un "creciente odio hacia Elon Musk en el personal".[10] Este tipo de ambiente puede erosionar la moral y el compromiso, creando un terreno fértil para las amenazas internas. La alta rotación de personal y la microgestión excesiva, según se informa, también contribuyen a un entorno que podría alentar a los empleados a convertirse en "turncloaks" o "revendedores de datos," vendiendo información confidencial a la competencia.[10] Esta situación trasciende las vulnerabilidades técnicas, ya que convierte la cultura corporativa en un vector de ataque primario.

2.3 Compromiso con la Gestión de Riesgos

La política de gestión de riesgos de SpaceX, según el marco de referencia, establece un compromiso con la provisión de los recursos necesarios para "blindar la organización" y "mitigar la materialización de los diferentes riesgos identificados".[5] Esta política destaca la necesidad de un personal cualificado para analizar, evaluar, tratar y monitorear los riesgos de manera constante.[5] Aunque la información no confirma la certificación de SpaceX en un esquema específico como ISO 27001, la estructura de la matriz de riesgos proporcionada se alinea con sus principios. En el contexto más amplio de la industria, la NASA ha emitido una guía de mejores prácticas de ciberseguridad para naves espaciales en 2023, que incluye principios como la protección contra el acceso no autorizado.[4] Sin embargo, la guía es opcional, lo que indica una posible falta de estándares de ciberseguridad obligatorios en la industria y subraya la necesidad de que SpaceX adopte proactivamente medidas robustas por sí misma.

3. Identificación y Valoración de Activos de Información

Los activos de información de SpaceX se valoran en función de tres criterios críticos: Confidencialidad (C), Integridad (I) y Disponibilidad (D). Una puntuación de 5 en cualquiera de estos criterios indica la máxima criticidad.

3.1 Planos de Cohetes y Diseños de Propulsión

Estos activos representan el corazón de la propiedad intelectual de SpaceX y su ventaja competitiva. El valor de este activo es máximo en todas las dimensiones. La confidencialidad es crítica, ya que el robo de diseños por parte de naciones adversarias o competidores puede causar daños económicos masivos y representar una amenaza a la seguridad nacional.[8] La integridad es crucial, pues la alteración maliciosa de un plano podría provocar un fallo catastrófico en una misión, con la consiguiente pérdida de la nave, la carga y potencialmente vidas humanas. La disponibilidad es vital para el desarrollo, la producción y el mantenimiento continuos.

- **Valoración:** Confidencialidad (C=5), Integridad (I=5), Disponibilidad (D=5).

3.2 Investigación y Modelos de Inteligencia Artificial (IA)

SpaceX utiliza IA en sistemas de propulsión, control de vuelo y otras tecnologías avanzadas. Estos modelos son un activo de alta criticidad, ya que su desarrollo es fundamental para los futuros esfuerzos de exploración espacial.[13] La integridad de los modelos de IA es de suma importancia; si los datos de entrenamiento son manipulados, los sistemas podrían aprender comportamientos erróneos, llevando a decisiones incorrectas o fallos en sistemas críticos.[15] La confidencialidad también es alta debido al valor comercial y estratégico de los modelos.

- **Valoración:** Confidencialidad (C=4), Integridad (I=5), Disponibilidad (D=4).

3.3 Credenciales de Sistemas y Agentes de IA

Las credenciales, especialmente las de acceso privilegiado, son el activo más crítico para la seguridad, ya que su compromiso puede otorgar acceso no autorizado a la totalidad de los sistemas y la información.[16] Su compromiso es el vector de ataque más común para las filtraciones de datos.[16] La confidencialidad de las credenciales es absoluta, su integridad es esencial para que solo los usuarios autorizados puedan operar, y su disponibilidad es necesaria para el funcionamiento diario.

- **Valoración:** Confidencialidad (C=5), Integridad (I=5), Disponibilidad (D=5).

3.4 Datos de Empleados y del Personal

Este activo, que incluye información personal y datos de RR. HH., es de alta criticidad debido a las graves implicaciones legales y de reputación en caso de una filtración.[17] Incidentes en otras empresas asociadas con el mismo liderazgo han expuesto datos de empleados, lo que subraya la vulnerabilidad de este activo.[18] La confidencialidad es la prioridad principal, y su disponibilidad es necesaria para las operaciones de recursos humanos. La pérdida de estos datos puede resultar en multas, demandas, robo de identidad y una pérdida de confianza de los empleados.[17]

- **Valoración:** Confidencialidad (C=5), Integridad (I=3), Disponibilidad (D=3).

4. Análisis Detallado de Riesgos por Activo

La siguiente tabla presenta un análisis detallado de los riesgos identificados para cada activo de información, siguiendo la estructura de la matriz de riesgos.

PROCESO / LÍDER	TIPO DE ACTIVO	NOMBRE DEL ACTIVO	AMENAZA	VULNERABILIDAD	DESCRIPCIÓN DEL RIESGO	POSIBLE CONSECUENCIA	NIVEL DEL RIESGO

Ingeniería de Cohetes	Datos/Información	Planos de Cohetes y Diseños de Propulsión	Ciberespionaje	Protección de la PI.	Robo de propiedad intelectual por actores de estado y competidores.	Pérdida de ventaja competitiva, impacto económico, amenaza a la seguridad nacional.	Catastrófico (60)
Recursos Humanos / Director	Datos/Información	Datos de Empleados y Personal	Amenazas internas	Cultura laboral hostil, falta de supervisión.	Filtración o venta de datos de empleados por personal descontento o negligente.	Demandas legales, multas, robo de identidad, daño a la reputación.	Catastrófico (60)
I&D / Director de IA	Datos/Información	Investigación y Modelos de IA	Manipulación de datos	Falta de controles de calidad.	Envenenamiento de los datos de entrenamiento de modelos de IA.	Fallo catastrófico en sistemas de control autónomo, pérdida de misione	Inaceptable (60)

						s y vidas.	
TI / CISO	Credenciales	Credenciales de Sistemas y Agentes de IA	Phishing dirigido	Falta de MFA, concienciа del usuario.	Compromiso de credenciales de alto privilegio a través de ingeniería social.	Acceso total a sistemas críticos, robo de todos los activos de información.	Catastrófico (60)
Ingeniería de Cohetes	Datos/Información	Planos de Cohetes y Diseños de Propulsión	Amenazas internas	Cultura de presión y descontento.	Sabotaje o filtración de información confidencial por empleados desmotivados.	Retrasos en misiones, fallos en lanzamientos, divulgación de secretos comerciales.	Catastrófico (60)
TI / CISO	Credenciales	Credenciales de Sistemas y Agentes de IA	Abuso de privilegios	Gestión de acceso deficiente.	Uso indebido de credenciales legítimas por empleados para fines	Exfiltración de datos sensibles, acceso no autorizado a sistemas	Catastrófico (60)

					malicios os.	críticos.	
I&D / Director de IA	Datos/I nforma ción	Investig ación y Modelo s de IA	Robo de PI	Vulnera bilidade s en la cadena de suminis tro de IA.	Robo de los modelo s y algorit mos de IA de propied ad de SpaceX .	Pérdida de ventaja competi tiva, daño económ ico, incumpl imiento de contrat os.	Inacept able (60)
I&D / Director de IA	Datos/I nforma ción	Investig ación y Modelo s de IA	Riesgos éticos	Falta de regulaci ón clara, uso de datos sesgad os.	Uso de datos de entrena miento sesgad os que pueden generar resulta dos injustos o discrimi natorio s.	Riesgos de cumpli miento normati vo, deman das, daño a la imagen corpora tiva.	Inacept able (60)
TI / CISO	Creden ciales	Creden ciales de Sistema s y Agente s de IA	Mala gestión del ciclo de vida	Proces os de desvinc ulación insegur os.	Cuenta s de ex-empl eados no desacti vadas,	Acceso persiste nte y malicios o a la red y a la	Catastr ófico (60)

					permitiendo acceso no autorizado.	información corporativa.	

4.1 Riesgos en Planos de Cohetes y Diseños de Propulsión

- **Riesgo 1: Ciberespionaje y Robo de Propiedad Intelectual.** La industria aeroespacial es un objetivo prioritario para el ciberespionaje, con el robo de propiedad intelectual siendo una amenaza persistente y bien financiada por actores de estado y competidores.[6] La vulnerabilidad de SpaceX reside en el alto valor de sus diseños de cohetes y la interconexión de sus servicios comerciales y gubernamentales a través de proyectos como Starshield, que atiende al DOD y otros socios de defensa.[3] Esto eleva el riesgo de un simple "robo de PI" a una "amenaza a la seguridad nacional," lo cual requiere un nivel de protección muy superior al de una empresa comercial promedio. La geoeconomía del ciberespionaje indica que el costo anual de este tipo de ataques puede ascender a billones de dólares.[8]
- **Riesgo 2: Filtración por Amenazas Internas Maliciosas o Negligentes.** Las denuncias de empleados sobre una cultura de trabajo hostil, la microgestión y el "creciente odio" hacia la dirección crean una vulnerabilidad significativa.[10] Un empleado que se siente maltratado o despreciado puede convertirse en una amenaza interna, vendiendo o divulgando información confidencial a la competencia o en la web oscura.[11] Este riesgo es particularmente insidioso porque las vulnerabilidades no son solo técnicas, sino que residen en el elemento humano. Las fallas en la gestión del personal se convierten en un vector de ataque directo, lo que demuestra que la seguridad en SpaceX debe ir de la mano con una mejora en el ambiente laboral.[12]
- **Riesgo 3: Infiltración a través de la Cadena de Suministro.** SpaceX depende de una vasta red de proveedores y socios para la fabricación y el ensamblaje de sus cohetes y naves.[5] Un ataque dirigido a uno de estos proveedores, que podría tener controles de seguridad más débiles, podría ser una puerta de entrada para acceder a los diseños o sistemas de SpaceX.

4.2 Riesgos en Investigación y Modelos de Inteligencia Artificial (IA)

- **Riesgo 1: Manipulación de Datos de Entrenamiento (Envenenamiento).** La integridad de los modelos de IA de SpaceX es de importancia crítica. Un adversario podría inyectar datos incorrectos o maliciosos en los vastos conjuntos de datos utilizados para el entrenamiento.[14] Esto podría llevar a que los modelos aprendan a operar con premisas defectuosas, lo que podría resultar en predicciones o clasificaciones incorrectas y, en el contexto de SpaceX, un fallo catastrófico en un sistema de control autónomo o en una misión espacial.[15] Este riesgo de integridad es tan vital como la confidencialidad y podría tener consecuencias devastadoras.
- **Riesgo 2: Robo de Propiedad Intelectual de los Modelos de IA.** Aparte de la manipulación, el robo de los modelos de IA y sus algoritmos es una amenaza latente.[21] Las vulnerabilidades en la cadena de suministro de IA o el uso de plataformas de terceros que podrían reutilizar los datos de entrenamiento de SpaceX representan un riesgo significativo para la confidencialidad de este activo.[14]
- **Riesgo 3: Riesgos de Cumplimiento y Ética.** La IA aún carece de un marco regulatorio claro.[13] SpaceX enfrenta el riesgo de utilizar datos sesgados para el entrenamiento de sus modelos, lo que podría dar lugar a resultados discriminatorios o injustos. El incumplimiento de futuras regulaciones de IA podría resultar en multas y daños a la reputación.[14]

4.3 Riesgos en Credenciales de Sistemas y Agentes de IA

- **Riesgo 1: Compromiso de Credenciales por Phishing Dirigido (Spear Phishing).** El phishing es la causa más común de violaciones de datos, y el spear phishing, que se dirige a individuos o grupos específicos, es particularmente efectivo.[23] Los atacantes pueden usar la ingeniería social para engañar a personal clave, como ingenieros o administradores de centros de datos, para que divulguen sus credenciales de acceso.[16] La falta de autenticación multifactor (MFA) en cuentas heredadas se ha identificado como una vulnerabilidad clave.[16]
- **Riesgo 2: Abuso de Credenciales por Amenazas Internas.** Incluso con credenciales legítimas, los empleados pueden abusar de sus privilegios para acceder a información o sistemas a los que no deberían.[11] Un ambiente laboral tenso puede motivar a los empleados a causar daño a la empresa.[10] Una gestión de acceso privilegiado (PAM) deficiente, sin controles de acceso "Just-in-Time" o auditorías periódicas, amplifica este riesgo.[26]
- **Riesgo 3: Mala Gestión del Ciclo de Vida de las Credenciales.** El posible alto índice de rotación de personal en SpaceX aumenta el riesgo de que las credenciales de ex-empleados no se desactiven adecuadamente, lo que podría dejar puertas traseras

abiertas para el acceso no autorizado.[10]

4.4 Riesgos en Datos de Empleados

- **Riesgo 1: Filtración Masiva de Datos Personales.** Las empresas lideradas por Elon Musk, como Twitter/X y Tesla, han sufrido filtraciones de datos personales masivas, exponiendo información de millones de usuarios y empleados.[18] Este patrón de incidentes sugiere una vulnerabilidad sistémica que podría manifestarse en SpaceX. La falta de medidas de seguridad robustas podría exponer información personal sensible, lo que puede resultar en robo de identidad y fraude.[20]
- **Riesgo 2: Daño Reputacional y Legal.** Una filtración de datos de empleados no solo tiene consecuencias económicas directas, sino que también puede generar un daño reputacional severo y una cascada de implicaciones legales.[17] El incumplimiento de regulaciones de protección de datos como el GDPR o la CCPA podría resultar en fuertes sanciones.[14]
- **Riesgo 3: Uso Indebido de Datos por Amenazas Internas.** Al igual que con los planos y diseños, el ambiente laboral podría incentivar a los empleados a convertirse en "revendedores de datos," vendiendo información personal de otros empleados, bases de datos de clientes, o secretos de la empresa a la competencia.[11]

5. Plan de Tratamiento de Riesgos y Controles Propuestos

5.1 Medidas de Reducción

Para mitigar los riesgos identificados, se propone la implementación de los siguientes controles, alineados con el Anexo A de la ISO 27001:

- **Para Planos de Cohetes:**
  - Implementar un sistema de gestión de derechos de información (IRM) y controles de acceso basados en roles (A.5.18, A.8.2).
  - Cifrar todos los datos de diseño tanto en tránsito como en reposo. Se debe

considerar el uso de la criptografía, por ejemplo, AES-256, para proteger la confidencialidad e integridad de los planos.[20]
    - Fortalecer el programa de concientización sobre amenazas internas, educando a los empleados sobre los riesgos del ciberespionaje y la importancia de reportar comportamientos sospechosos (A.6.3).
- **Para Investigación de IA:**
    - Desarrollar un marco de gobernanza de datos para la IA que incluya la validación de la calidad de los datos de entrenamiento y el monitoreo continuo de los modelos de IA para detectar desviaciones o degradación del rendimiento (A.8.25).
    - Proteger los datos y modelos de la IA en toda la cadena de suministro para evitar ataques de envenenamiento o robo.[14]
- **Para Credenciales:**
    - Implementar la autenticación multifactor (MFA) de manera obligatoria para todas las cuentas, especialmente las privilegiadas, para proteger contra ataques de phishing.[16]
    - Usar una solución de gestión de acceso privilegiado (PAM) con acceso "Just-in-Time" para cuentas críticas, lo que revoca los privilegios después de un período de tiempo definido.[26]
    - Mejorar los procesos de desvinculación para garantizar que las credenciales de los empleados salientes se deshabiliten de inmediato y se realicen auditorías de acceso (A.5.12).
- **Para Datos de Empleados:**
    - Fortalecer las políticas de protección de datos y la gestión del acceso, asegurando que solo el personal autorizado tenga acceso a la información personal de los empleados (A.5.15).
    - Realizar auditorías periódicas para identificar el acceso no autorizado y las vulnerabilidades.[17]
    - Establecer un plan de respuesta a incidentes de seguridad que incluya la notificación a las autoridades y a los afectados en caso de una filtración.[17]

5.2 Acciones de Transferencia y Aceptación

Además de la reducción, se debe considerar la transferencia de riesgos a través de seguros cibernéticos que cubran las pérdidas financieras y los costos legales asociados con las filtraciones de datos y las interrupciones del negocio. Por último, se debe documentar y aceptar formalmente cualquier riesgo residual que, después de la implementación de los controles, se considere tolerable.[5]

6. Conclusiones y Futuras Implicaciones

6.1 Síntesis de la Postura de Seguridad

El análisis de la matriz de riesgos de SpaceX revela que la seguridad de la información es una disciplina multifacética que no puede limitarse a la implementación de tecnología de vanguardia. Si bien los activos de la empresa son de alto valor estratégico y técnico, las vulnerabilidades más críticas se encuentran en la intersección de factores humanos y organizacionales. Las tensiones internas reportadas y la historia de filtraciones en empresas del mismo liderazgo sugieren que SpaceX debe abordar las causas fundamentales de la desmotivación del personal y la cultura de seguridad para mitigar el riesgo interno.

6.2 Implicaciones a Largo Plazo y Propuestas de Mejora Continua

Ignorar los riesgos organizacionales y humanos podría tener consecuencias catastróficas a largo plazo, no solo en términos de pérdidas financieras, sino también en el fracaso de misiones y la erosión de la confianza pública y gubernamental. La naturaleza de los activos de SpaceX, combinada con su papel en la seguridad nacional, exige una postura de seguridad que sea proactiva e integral. Se recomienda a la alta dirección la adopción de un enfoque holístico que considere la seguridad no como una carga, sino como un pilar fundamental para el éxito y la sostenibilidad de su misión. La inversión en la capacitación continua del personal, el fortalecimiento de los controles de acceso privilegiado y la implementación de un robusto marco de gobernanza de la IA son pasos cruciales para blindar a la organización contra las amenazas emergentes y garantizar que el futuro multiplanetario de la humanidad se construya sobre una base de seguridad sólida.

Works cited

1. Declaración de misión y visión de SpaceX - Business Model Analyst, accessed August 21, 2025, https://businessmodelanalyst.com/es/declaraci%C3%B3n-de-misi%C3%B3n-y-visi%C3%B3n-de-spacex/
2. SpaceX, accessed August 21, 2025, https://www.spacex.com/
3. SpaceX differentiates between Starlink and Starshield, but the services are intertwined, accessed August 21, 2025,

https://fedscoop.com/spacex-starlink-starshield-government-military-satellite-internet/
4. NASA Cybersecurity: Plan Needed to Update Spacecraft Acquisition Policies and Standards, accessed August 21, 2025, https://www.gao.gov/products/gao-24-106624
5. 1. Matriz de riesgos 27001
6. Los ciberataques contra el sector de la aviación incrementan en un 600% en el último año, accessed August 21, 2025, https://www.revistaejercitos.com/noticias-de-industria-de-defensa/los-ciberataques-contra-el-sector-de-la-aviacion-incrementan-en-un-600-en-el-ultimo-ano/
7. Conferencia de prensa en línea: ESET descubre ciberespionaje en la industria aeroespacial - Somos Uruguay, accessed August 21, 2025, https://somosuruguay.com.uy/empresariales/conferencia-prensa-linea-eset-descubre-ciberespionaje-industria-aeroespacial-n429
8. El robo de propiedad intelectual roba las ideas más brillantes de Estados Unidos, accessed August 21, 2025, https://www.iwf.org/es/2022/04/26/intellectual-property-theft/
9. Data Center Administrator @ SpaceX | Thrive Capital Job Board, accessed August 21, 2025, https://jobs.thrivecap.com/companies/spacex/jobs/57015655-data-center-administrator
10. Empleados de SpaceX denuncian el DESCONTROL TOTAL en Starbase - YouTube, accessed August 21, 2025, https://www.youtube.com/watch?v=IeExDPr0FSI
11. ¿Qué es una amenaza interna? Definición, ejemplos y solución - Safetica, accessed August 21, 2025, https://www.safetica.com/es/recursos/blogs/que-es-una-amenaza-interna-definicion-ejemplos-y-solucion
12. ¿Qué es una amenaza interna? Definición, tipos y prevención - Fortinet, accessed August 21, 2025, https://www.fortinet.com/lat/resources/cyberglossary/insider-threats
13. 9 riesgos en la Inteligencia Artificial y cómo gestionarlos - Pirani, accessed August 21, 2025, https://www.piranirisk.com/es/blog/9-riesgos-en-la-inteligencia-artificial-y-como-gestionarlos
14. ¿Qué es la seguridad de IA? - IBM, accessed August 21, 2025, https://www.ibm.com/mx-es/think/topics/ai-security
15. ¿Qué es el entrenamiento de modelos de IA y por qué es importante? | Oracle Argentina, accessed August 21, 2025, https://www.oracle.com/ar/artificial-intelligence/ai-model-training/
16. ¿Qué es una credencial comprometida? | Silverfort Glosario, accessed August 21, 2025, https://www.silverfort.com/es/glossary/compromised-credential/
17. Brechas de seguridad de datos personales: qué son y cómo actuar | AEPD, accessed August 21, 2025, https://www.aepd.es/prensa-y-comunicacion/blog/brechas-de-seguridad-de-datos-personales-que-son-y-como-actuar

18. Otra chapuza de Elon Musk: una filtración de datos afectaría al 50% de los usuarios de Twitter - El Confidencial, accessed August 21, 2025, https://www.elconfidencial.com/tecnologia/2025-04-02/filtracion-50-por-ciento-usuarios-twitter-1qrt_4099983/
19. Filtración de datos privados en Tesla | INCIBE-CERT, accessed August 21, 2025, https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/filtracion-de-datos-privados-en-tesla
20. ¿Qué es la seguridad de los datos? - Microsoft, accessed August 21, 2025, https://www.microsoft.com/es-mx/security/business/security-101/what-is-data-security
21. Las empresas de IA están cometiendo el mayor robo de propiedad intelectual, acusa senador estadounidense | DPL News, accessed August 21, 2025, https://dplnews.com/las-empresas-de-ia-estan-cometiendo-el-mayor-robo-de-propiedad-intelectual-acusa-senador-estadounidense/
22. ¿Cómo funciona el entrenamiento de modelos de IA? - Appian, accessed August 21, 2025, https://appian.com/es/blog/acp/ai/how-does-ai-model-training-work
23. www.ibm.com, accessed August 21, 2025, https://www.ibm.com/es-es/think/topics/spear-phishing#:~:text=Los%20ataques%20de%20spear%20phishing,com%C3%BAn%20de%20vulneraciones%20de%20datos.
24. ¿Qué es spear phishing? - IBM, accessed August 21, 2025, https://www.ibm.com/es-es/think/topics/spear-phishing
25. Incidente de Twitter: empleados fueron engañados vía phishing telefónico - WeLiveSecurity, accessed August 21, 2025, https://www.welivesecurity.com/la-es/2020/08/03/incidente-seguridad-twitter-empleados-enganados-phishing-telefonico/
26. Gestión de cuentas privilegiadas - Privileged Access Management | Proofpoint ES, accessed August 21, 2025, https://www.proofpoint.com/es/threat-reference/privileged-access-management-pam