Revista Científica Multidisciplinar G-ner@ndo ISSN: 2806-5905

Aseguramiento del Ciclo de Vida de Datos en la Industria 4.0: Metodología y Análisis Comparativo de Riesgos y Controles frente al Sector Financiero.

Data Lifecycle Assurance in Industry 4.0: Methodology and Comparative Analysis of Risks and Controls Compared to the Financial Sector.

Publio Ponce Palma & Edwin Patricio Camino Zambrano.

PUNTO CIENCIA.

Julio - diciembre, V°6 - N°2; 2025

Recibido: 15-08-2025
Aceptado: 15-08-2025
Publicado: 30-12-2025

PAIS

- Ecuador, Santo Domingo de los Colorados
- Ecuador, Sangolquí

INSTITUCION

- Escuela Superior Politécnica del Litoral.
- Universidad de las Fuerzas Armadas ESPE

CORREO:

✉ peponce@espol.edu.ec
✉ epcamino@espe.edu.ec

ORCID:

https://orcid.org/0009-0003-1669-7703
https://orcid.org/0000-0001-7799-5729

FORMATO DE CITA APA.

Ponce, P. & Camino, E. (2025). Aseguramiento del Ciclo de Vida de Datos en la Industria 4.0: Metodología y Análisis Comparativo de Riesgos y Controles frente al Sector Financiero. *Revista G-ner@ndo, V°6 (N°2). Pág. 928 –957.*

Resumen

La Industria 4.0, mediante la convergencia de Tecnologías de la Información (IT) y Tecnologías de Operación (OT), introduce beneficios significativos, pero también complejos desafíos de ciberseguridad. Este artículo analiza integralmente los riesgos a lo largo del ciclo de vida del dato industrial, desde la generación en planta (OT) hasta su transporte (ETL), almacenamiento (IT/Cloud) y consumo (BI/Apps). Utilizando un marco metodológico que incluye revisión de literatura, estándares (ej. ISO 50001) y un análisis comparativo con el sector financiero, se identifican vulnerabilidades clave en cada etapa, como sistemas OT legados, comunicaciones inseguras, configuraciones débiles y riesgos en aplicaciones low-code. La discusión resalta las diferencias fundamentales en prioridades (Disponibilidad en OT vs. Confidencialidad e Integridad en Finanzas) y la necesidad de adaptar controles. Se concluye que una estrategia de ciberseguridad holística, basada en riesgos y contextualizada al entorno industrial, es indispensable no solo para mitigar amenazas, sino como un habilitador esencial para el éxito seguro de la transformación digital industrial.

Palabras clave: Ciberseguridad Industrial, Industria 4.0. Seguridad OT, Ciclo de Vida del Dato, ISO 50001.

Abstract

Industry 4.0, through the convergence of Information Technology (IT) and Operational Technology (OT), introduces significant benefits, but also complex cybersecurity challenges. This paper comprehensively analyzes the risks across the industrial data lifecycle, from plant-floor generation (OT) through transport (ETL), storage (IT/Cloud), and consumption (BI/Apps). Using a methodological framework including literature review, standards (e.g., ISO 50001), and a comparative analysis with the financial sector, key vulnerabilities are identified at each stage, such as legacy OT systems, insecure communications, weak configurations, and low-code application risks. The discussion highlights fundamental differences in priorities (Availability in OT vs. Confidentiality and Integrity in Finance) and the need for adapted controls. It concludes that a holistic, risk-based, and context-aware cybersecurity strategy, tailored to the industrial environment, is indispensable not only for mitigating threats but also as a critical enabler for the secure success of the industrial digital transformation.

Keywords: Industrial Cybersecurity, Industry 4.0, OT Security, Data Lifecycle, ISO 50001.

Introducción

La Transformación Digital Industrial (Industria 4.0)

El panorama industrial global se encuentra inmerso en una profunda transformación, comúnmente denominada la Cuarta Revolución Industrial o Industria 4.0. Este paradigma emergente se caracteriza por la integración sistémica de tecnologías digitales avanzadas – como el Internet Industrial de las Cosas (IIoT), el análisis de Big Data, la Inteligencia Artificial (IA), la computación en la nube y los sistemas ciberfísicos (CPS) – en los procesos de producción y las cadenas de valor (Andrango Alobuela & Arroyo Morocho, 2022). Las organizaciones adoptan la Industria 4.0 con el objetivo de alcanzar niveles sin precedentes de eficiencia operativa, agilidad productiva, mantenimiento predictivo basado en datos, y una optimización sustancial de recursos, incluyendo la gestión energética, a menudo guiada por estándares como la ISO 50001. En este nuevo ecosistema industrial, los datos se convierten en el activo fundamental, el "combustible" que impulsa la toma de decisiones inteligentes y la automatización avanzada. Se generan volúmenes masivos de información heterogénea en tiempo real, desde lecturas de sensores (eléctricos, térmicos, de vibración, presión) y parámetros de control de maquinaria (PLCs, SCADA), hasta métricas de producción (MES), calidad y logística (ERP), cuyo valor estratégico reside en su capacidad para ser transformados en conocimiento accionable.

El Desafío de la Ciberseguridad en la Convergencia IT/OT

La convergencia entre tecnologías de la información (IT) y tecnologías operativas (OT) introduce nuevos desafíos de ciberseguridad. García Núñez (2023) destaca que el análisis y refuerzo de vulnerabilidades en estos entornos son esenciales para proteger infraestructuras críticas frente a ataques dirigidos, proponiendo estrategias prácticas para mitigar riesgos. Históricamente, los sistemas de Tecnología Operacional (OT) – responsables del monitoreo y control directo de procesos físicos industriales – operaban

en entornos aislados, desconectados de las redes corporativas de Tecnología de la Información (IT). La prioridad absoluta en OT ha sido tradicionalmente la disponibilidad, la fiabilidad y la seguridad física, con ciclos de vida de los equipos muy largos y protocolos de comunicación a menudo propietarios o inseguros por diseño. Por el contrario, el mundo IT ha priorizado la confidencialidad, integridad y disponibilidad (la tríada CIA) de la información, desarrollando robustas prácticas de seguridad para proteger datos y sistemas en redes interconectadas. La Industria 4.0 rompe radicalmente esta separación, exigiendo una interconexión fluida entre los mundos OT e IT para permitir el flujo de datos desde la planta hacia sistemas de análisis centralizados o en la nube. Esta convergencia IT/OT, si bien habilitadora de enormes beneficios, expande drásticamente la superficie de ataque, exponiendo sistemas OT críticos a un abanico de ciberamenazas antes desconocido en esos entornos. Las consecuencias de un ciberataque exitoso en la industria van más allá de la pérdida financiera o el robo de datos típicos del mundo IT; pueden incluir la interrupción o paralización total de la producción, daños físicos a maquinaria costosa, incidentes medioambientales, la alteración de procesos que comprometa la calidad del producto y, en el peor de los casos, riesgos directos para la seguridad y la vida humana.

El Problema: Asegurar el Flujo Completo de Datos Industriales

Ante esta nueva realidad, asegurar los activos industriales requiere una perspectiva que trascienda la protección de componentes individuales. La seguridad de la información en entornos de tecnologías operativas (OT) es crucial para proteger infraestructuras críticas. (López Prieto et al. ,2022) proponen la adopción de buenas prácticas en seguridad de la información, como la implementación de controles específicos y la capacitación del personal, para mitigar riesgos en ambientes OT. Es imperativo proteger la integridad, confidencialidad y disponibilidad de los datos a lo largo de todo su ciclo de vida dentro del ecosistema industrial conectado. Este ciclo abarca desde la generación inicial en sensores y controladores (PLCs) en la planta; su

agregación y transporte a través de redes OT, gateways IIoT y procesos de ETL, a menudo implementados con herramientas como Python; el almacenamiento seguro en bases de datos históricas, bases de datos relacionales o NoSQL, y Data Lakes, ya sea on-premise o en la nube; el procesamiento y análisis utilizando plataformas de Big Data o servicios cloud; hasta la visualización y acción, donde los insights se presentan en herramientas de Business Intelligence o se utilizan para alimentar aplicaciones de negocio o plataformas de bajo código (como Power Platform) que pueden incluso interactuar de nuevo con los sistemas de control. Una vulnerabilidad en cualquiera de estas etapas puede comprometer toda la cadena: datos de sensores manipulados pueden llevar a decisiones operativas erróneas, una brecha durante el almacenamiento puede exponer propiedad intelectual crítica, y un acceso no autorizado a través de una aplicación de visualización puede revelar información estratégica de producción. Por lo tanto, la ciberseguridad en la Industria 4.0 exige un enfoque holístico y resiliente que garantice la protección de los datos "desde el sensor hasta la nube" (ISA Global Cybersecurity Alliance [ISAGCA], 2020).

Enfoque Comparativo: Lecciones del Sector Financiero

Para abordar la complejidad de la seguridad en la Industria 4.0, este artículo adopta un enfoque comparativo, utilizando el sector financiero como punto de referencia. Este sector, se caracteriza por una alta madurez en ciberseguridad IT, impulsada por décadas de enfrentar amenazas sofisticadas y un entorno regulatorio extremadamente exigente que prioriza la protección de activos monetarios y datos personales identificables (Ghelani et al., 2022). Si bien las prioridades fundamentales difieren – el sector financiero pone un énfasis primordial en la Confidencialidad e Integridad, mientras que en OT industrial la Disponibilidad y la Integridad operacional suelen tener precedencia – el análisis de las prácticas financieras ofrece un prisma valioso. Estudiar cómo el sector financiero aborda el ciclo de vida de desarrollo seguro de software (incluyendo CI/CD con herramientas como Jenkins), la gestión de identidades y

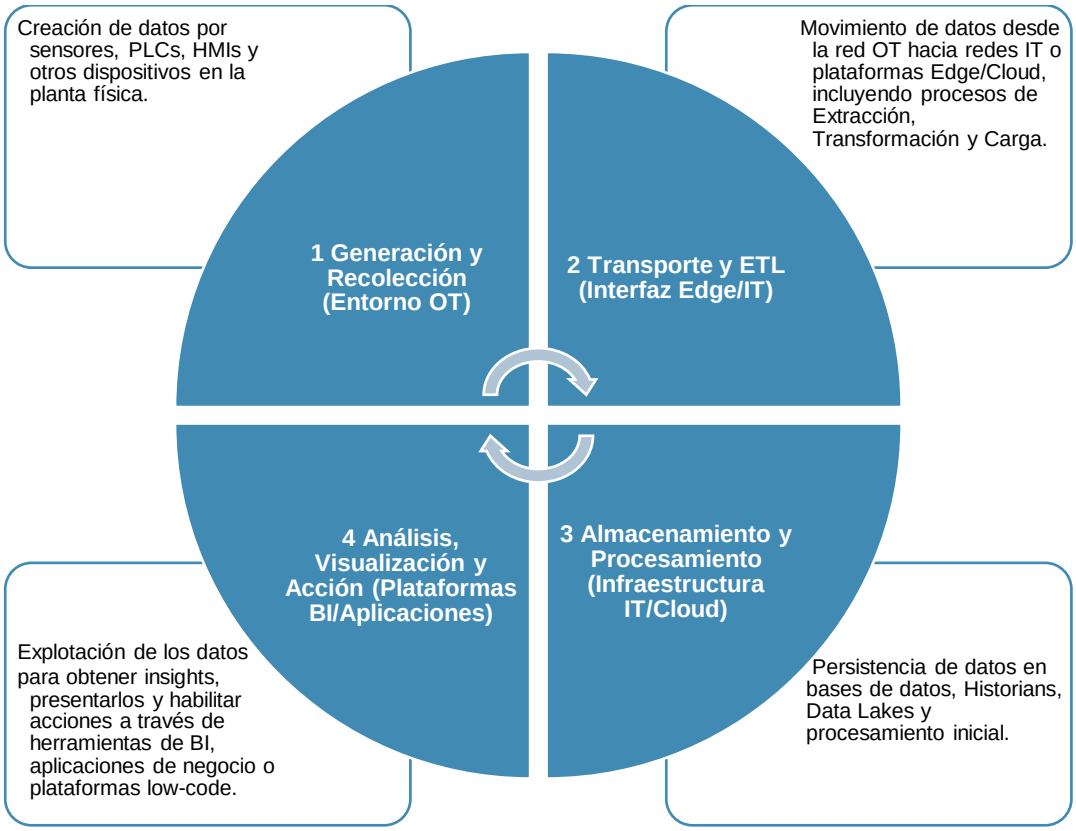
accesos, la segmentación de redes, la respuesta a incidentes y el cumplimiento normativo puede revelar estrategias adaptables o, por el contrario, resaltar las brechas donde el contexto OT requiere soluciones fundamentalmente diferentes debido a sus sistemas legados, protocolos específicos y tolerancia al riesgo operacional. Esta perspectiva comparativa, fundamentada en la experiencia multi-sectorial del autor, permite una evaluación más rica y matizada de los desafíos y soluciones para la ciberseguridad industrial.

Métodos y Materiales

Marco de Análisis: Ciclo de Vida del Dato Industrial

Para analizar de manera estructurada los riesgos de ciberseguridad en entornos de Industria 4.0, se ha definido un marco conceptual basado en las etapas clave del ciclo de vida de los datos industriales. Este marco permite seguir el flujo continuo de información desde su origen hasta su utilización final, identificando puntos críticos de vulnerabilidad en cada fase (Belman-López et al, 2023). Las etapas consideradas en este estudio son:

Figura 1.



Estándares

Se realizó una revisión sistemática de diversas fuentes para fundamentar el análisis. El estudio se apoya en estándares y marcos de referencia clave en ciberseguridad y gestión, tales como:

- ISA/IEC 62443: Serie de estándares fundamental para la seguridad en sistemas de automatización y control industrial (IACS). (International Society of Automation & International Electrotechnical Commission, 2018).

- NIST Cybersecurity Framework (CSF): Marco ampliamente adoptado para la gestión del riesgo de ciberseguridad en infraestructuras críticas. (National Institute of Standards and Technology, 2024).

- ISO/IEC 27001: Estándares internacionales para la gestión de la seguridad de la información (International Organization for Standardization & International Electrotechnical Commission, 2022).

- Normativas y estándares financieros relevantes (para comparación): Como los principios de seguridad asociados a PCI-DSS, regulaciones bancarias específicas sobre ciberseguridad y resiliencia operacional, y estándares de mensajería como ISO 20022 (International Organization for Standardization, 2013).

- ISO 50001: Estándar de gestión de la energía, relevante para contextualizar la importancia de la integridad de los datos energéticos analizados. (International Organization for Standardization, 2018).

Metodología de Identificación y Evaluación de Riesgos

La identificación de riesgos de ciberseguridad para cada etapa del ciclo de vida del dato se realizó mediante un proceso analítico. Se identificaron los activos de información críticos en cada fase, se analizaron las vulnerabilidades típicas asociadas a las tecnologías y procesos involucrados y se consideraron las amenazas relevantes. La evaluación del riesgo se abordó de manera cualitativa, considerando la probabilidad estimada de ocurrencia (basada en la prevalencia de amenazas y vulnerabilidades) y el impacto potencial en el contexto industrial (considerando aspectos de producción,

seguridad operacional, financieros y reputacionales). Se aplicaron conceptualmente principios de modelado de amenazas, como la identificación de posibles puntos de fallo y vectores de ataque, sin realizar un modelado formal exhaustivo o una evaluación cuantitativa.

Metodología de Análisis Comparativo (Industria vs. Finanzas)

El análisis comparativo entre el sector industrial (enfocado en Industria 4.0) y el sector financiero se realizó con el objetivo de resaltar las diferencias contextuales clave y extraer posibles aprendizajes. La comparación se estructuró en torno a criterios específicos, incluyendo:

- Prioridades relativas de Confidencialidad, Integridad y Disponibilidad (Tríada CIA).
- Naturaleza de los activos críticos y datos sensibles protegidos.
- Panorama de amenazas predominante y perfil de los actores de amenaza.
- Características del entorno tecnológico (heterogeneidad, sistemas legados vs. modernos).
- Madurez y enfoque del marco regulatorio y de cumplimiento.
- Adopción y adaptación de controles y arquitecturas de seguridad.

Contexto Tecnológico

El análisis y la discusión presentados en la Sección 3 se informan considerando la seguridad de un espectro representativo de tecnologías comúnmente encontradas en los entornos estudiados. Estas incluyen, entre otras:

- Herramientas de ETL, análisis de datos y scripting, como Python y sus librerías asociadas.
- Plataformas de Business Intelligence y visualización de datos, como Power BI y GridVis.
- Plataformas de desarrollo low-code/no-code, como Microsoft Power Platform (Power Apps, Power Automate) y sistemas de gestión de contenido como SharePoint.
- Entornos de desarrollo de aplicaciones empresariales y financieras basados en lenguajes como Java.
- Sistemas de gestión de bases de datos relacionales y no relacionales, con énfasis en sistemas como Oracle y MSSql
- Herramientas de automatización de integración y entrega continua (CI/CD), como Jenkins, en contextos de desarrollo de software.
- Estándares de comunicación y mensajería financiera, como ISO 20022 y Swift.
- Conceptos generales de protocolos de comunicación industrial (ej., Modbus TCP, OPC-UA) y componentes de sistemas de control (PLCs, SCADA).

Principio de Pareto como Herramienta Conceptual

La optimización de recursos es un aspecto clave en la gestión empresarial moderna. Según Belmar Muñoz (2024), el principio de Pareto, también conocido como criterio 80-20, sugiere que "el 80% de los resultados en una empresa suelen provenir del 20% de los esfuerzos o recursos" (p. 3). Esta idea permite a las organizaciones priorizar actividades de alto impacto, como la mejora de procesos críticos, para

maximizar la eficiencia, por lo tanto, se utilizará el Principio de Pareto como una herramienta conceptual a lo largo del análisis en la Sección 3. Este principio ayuda a enmarcar la discusión sobre la priorización, sugiriendo que un número relativamente pequeño de activos, vulnerabilidades o puntos de control (los "pocos vitales") pueden ser responsables de la mayoría del riesgo o, inversamente, ofrecer el mayor retorno en la inversión en seguridad. La norma ISO 50001:2018 (International Organization for Standardization, 2018) establece un marco para implementar sistemas de gestión de energía que ayudan a las organizaciones a monitorear y reducir su consumo energético. Esto resuena con enfoques prácticos como la identificación de Usos Significativos de la Energía (USEs) en la gestión energética, aplicando una lógica similar a la gestión del riesgo cibernético.

Análisis de resultados

Etapa 1: Generación y Recolección de Datos (Entorno OT)

Descripción de la Etapa y Activos Clave

Esta primera etapa ocurre directamente en la planta de producción o el entorno físico industrial, el corazón de la Tecnología Operacional (OT). Aquí es donde los datos nacen, capturados por una variedad de dispositivos que interactúan directamente con los procesos físicos. Los activos clave incluyen:

- Sensores y Actuadores: Dispositivos finales que miden variables físicas (temperatura, presión, flujo, nivel, vibración - datos eléctricos, térmicos) o ejecutan acciones físicas (abrir/cerrar válvulas, mover motores). Cada vez más, estos son dispositivos "inteligentes" conectados en red (IIoT).

- Controladores Lógicos Programables (PLCs) y Unidades Terminales Remotas (RTUs): Cerebros de la automatización local que ejecutan la lógica

de control basada en las entradas de los sensores y comandan los actuadores.

- Interfaces Hombre-Máquina (HMIs): Pantallas locales que permiten a los operadores monitorizar y, en ocasiones, interactuar con el proceso controlado por los PLCs/RTUs.

- Sistemas de Control Distribuido (DCS) y Sistemas de Supervisión, Control y Adquisición de Datos (SCADA): Sistemas más complejos que gestionan y supervisan procesos a mayor escala, recopilando datos de múltiples PLCs/RTUs y proporcionando una visión centralizada.

Resultados: Vulnerabilidades y Amenazas Identificadas

El entorno OT presenta un conjunto único de vulnerabilidades, a menudo derivadas de su diseño histórico centrado en la fiabilidad y el aislamiento, no en la seguridad frente a ciberataques modernos:

- Sistemas Operativos y Firmware Obsoletos/Sin Parches: Muchos dispositivos OT (PLCs, HMIs, servidores SCADA) operan con sistemas operativos embebidos o versiones comerciales (ej. Windows 7, Server 2003/2008) que ya no reciben actualizaciones de seguridad del fabricante.

- Protocolos de Comunicación Inseguros: Protocolos industriales ampliamente utilizados (ej. Modbus TCP, DNP3 sin autenticación, S7comm) carecen de mecanismos inherentes de autenticación, cifrado o integridad, siendo susceptibles a escucha, manipulación de comandos o ataques de repetición.

- Credenciales Débiles o por Defecto: Es común encontrar dispositivos OT configurados con contraseñas de fábrica o credenciales fácilmente adivinables, facilitando el acceso no autorizado.

- Falta de Segmentación de Red: Históricamente, las redes OT eran planas. Aunque la segmentación está mejorando, aún existen redes donde un compromiso en un punto puede propagarse fácilmente a otros sistemas críticos.

- Acceso Físico Inseguro: En algunas instalaciones, el acceso físico a paneles de control, gabinetes de red o dispositivos OT puede no estar suficientemente restringido.

- Configuraciones Inseguras: Habilitación de servicios innecesarios (ej. FTP, Telnet), falta de hardening de los sistemas operativos subyacentes.

- Vulnerabilidades en Software de Control: El propio software SCADA/HMI/PLC puede contener vulnerabilidades explotables.

Las amenazas que explotan estas vulnerabilidades incluyen:

- Malware Específico para OT: Como Stuxnet, Industroyer, Triton, diseñados para manipular procesos físicos o causar daño.

- Acceso Remoto No Autorizado: A través de conexiones de mantenimiento inseguras.

- Ataques de Ingeniería Social: Dirigidos a ingenieros de control o personal de mantenimiento para obtener credenciales o instalar malware.

- Amenazas Internas: Empleados descontentos o errores humanos no intencionados.

- Interrupción del Servicio (DoS): Ataques que buscan sobrecargar dispositivos o redes OT para detener procesos.

- Manipulación de Datos/Comandos: Alterar lecturas de sensores o comandos a actuadores para sabotear la producción, comprometer la calidad o causar condiciones inseguras.

Discusión: Impacto, Análisis Comparativo y Mitigación

El impacto de un ciberataque exitoso en esta etapa puede ser devastador y va mucho más allá de la pérdida de datos. Incluye la parada total de la producción, daños a equipos costosos, liberación de materiales peligrosos al medio ambiente, y la producción de bienes defectuosos que pueden generar retiradas del mercado o daños al consumidor, mientras en una transacción financiera (asegurada, por ejemplo, con aplicaciones Java y protocolos como ISO 20022) la Confidencialidad de los datos del cliente y la Integridad de la transacción son primordiales, en el control de planta (OT), la Disponibilidad del proceso y la Integridad operacional suelen ser las máximas prioridades. Unos pocos segundos de indisponibilidad en OT pueden ser catastróficos, mientras que, en finanzas, a veces se puede sacrificar disponibilidad momentánea por seguridad.

Tabla 1.

Análisis Comparativo (vs. Sector Financiero).

Comparativo	Industria	Finanzas
Ciclo de vida del dato	Los ciclos de vida superan fácilmente los 10-15 años. El parcheo es un desafío inmenso, no solo por las ventanas de mantenimiento limitadas y el riesgo de interrumpir operaciones 24/7, sino también, como se mencionó anteriormente, por **la dependencia de software de control especializado con licencias costosas vinculadas a sistemas operativos específicos y obsoletos**.	Suelen tener ciclos de vida más cortos y procesos de parcheo ágiles, a menudo integrados en pipelines **CI/CD** (como con **Jenkins**).
Actualizaciones de sistemas	La migración de este software crítico a plataformas modernas representa una **barrera económica y técnica significativa**, perpetuando la existencia de sistemas vulnerables.	La modernización de los sistemas tecnológicos está intrínsecamente vinculada al desarrollo continuo de las herramientas de tecnologías de la información (TI). Este avance impulsa actualizaciones frecuentes en los sistemas

Dada la dificultad del parcheo y la naturaleza de los sistemas OT, las estrategias de mitigación se centran en la defensa en profundidad y la compensación de controles:

- Hardening de Sistemas: Deshabilitar servicios innecesarios, cambiar credenciales por defecto, configurar listas de control de acceso (ACLs) en dispositivos que lo permitan.

- Control de Acceso Físico y Lógico: Asegurar el acceso físico a los equipos e implementar autenticación robusta para el acceso lógico.

- Monitorización de Red OT Pasiva: Utilizar herramientas que escuchen el tráfico de red sin interactuar activamente, para detectar anomalías, uso de protocolos inseguros o firmas de malware OT específico.

- Gestión Segura de Acceso Remoto: Implementar soluciones de acceso remoto seguro (ej. VPNs con MFA, jump hosts en una DMZ industrial) con políticas estrictas y monitorización.

- Whitelisting de Aplicaciones: En estaciones de trabajo o servidores HMI/SCADA, permitir solo la ejecución de aplicaciones autorizadas.

- Planes de Respuesta a Incidentes Específicos para OT: Que consideren la contención en redes OT, la restauración segura de operaciones y la coordinación con equipos de seguridad física y operaciones.

Etapa 2: Transporte y ETL

Descripción de la Etapa y Activos Clave

Una vez generados los datos en la capa OT, esta segunda etapa se encarga de moverlos hacia entornos donde puedan ser almacenados, procesados y analizados más a fondo, típicamente las redes IT corporativas o plataformas en la nube. Actúa como un puente crucial entre el mundo físico (OT) y el digital (IT). Los activos clave en esta fase incluyen:

- Redes de Comunicación: Segmentos de red industrial (a menudo basados en Ethernet industrial), redes corporativas IT y conexiones WAN hacia la nube.

- Servidores y Plataformas ETL: Sistemas que ejecutan los procesos de Extracción (de fuentes OT o bases de datos intermedias), Transformación (limpieza, normalización, enriquecimiento) y Carga (hacia bases de datos o data warehouses). Estos procesos son frecuentemente implementados mediante scripts personalizados (por ejemplo, en Python) o herramientas ETL dedicadas.

- Firewalls y Dispositivos de Seguridad Perimetral: Controlan el flujo de tráfico entre las zonas OT e IT

Resultados: Vulnerabilidades y Amenazas Identificadas

Los riesgos en esta etapa se centran en la seguridad de la comunicación, la integridad de los datos durante la transformación y la seguridad de los sistemas intermediarios:

- Comunicaciones No Cifradas: Muchos protocolos OT no son cifrados, y si la comunicación hacia IT/Cloud tampoco se cifra adecuadamente, los datos pueden ser interceptados.

- Autenticación Débil o Ausente: Falta de autenticación robusta entre dispositivos OT, gateways y sistemas IT/Cloud, permitiendo conexiones no autorizadas o suplantación de identidad (spoofing).

- Gateways y Dispositivos Edge Inseguros: Configuraciones por defecto, firmware no actualizado, gestión de credenciales pobre, servicios de red innecesarios habilitados.

- Código Inseguro: Scripts ETL pueden tener vulnerabilidades como manejo inadecuado de entradas (permitiendo inyecciones), gestión insegura de errores que revela información, o lógica de transformación defectuosa que corrompe los datos.

- Gestión Insegura de Secretos: Credenciales de bases de datos u otros embebidas en el código o archivos de configuración no protegidos.

- APIs Inseguras: Si los datos se exponen o consumen a través de APIs, estas pueden carecer de autenticación/autorización adecuadas, limitación de tasa (rate limiting), o validación de entradas.

Las amenazas principales en esta fase pueden ser: Ataques Man-in-the-Middle (MitM), escucha de Red (Sniffing), manipulación/Inyección de Datos, denegación de servicio (DoS) o explotación de vulnerabilidades

Discusión: Impacto, Análisis Comparativo y Mitigación

El impacto de un fallo de seguridad en esta etapa es significativo porque puede corromper o exponer los datos antes de que lleguen a los sistemas de análisis y toma de decisiones. La pérdida de integridad aquí puede llevar a análisis erróneos, informes incorrectos (afectando, por ejemplo, el cálculo del desempeño energético para ISO 50001), alarmas falsas o la ausencia de alarmas verdaderas, y potencialmente a la toma de decisiones operativas o de negocio basadas en información falsa.

Tabla 2.

Análisis Comparativo (vs. Sector Financiero):

Comparativo	Industria	Finanzas
Seguridad en Tránsito	Asegurar la comunicación desde OT a menudo requiere añadir capas de seguridad (VPNs, TLS) sobre protocolos inherentemente inseguros, lo cual puede ser complejo de implementar y gestionar en entornos industriales.	depende de redes y protocolos con seguridad incorporada o muy robusta para mover fondos e información sensible
Seguridad de APIs	La adopción de APIs seguras para la integración industrial está menos madura, aunque creciendo con estándares como OPC-UA	Ha avanzado mucho en APIs seguras y robustas
Desarrollo Seguro ETL vs. Aplicaciones Financieras	No se aplican con el mismo nivel de formalidad o herramientas, especialmente si son desarrollados internamente por equipos de automatización o análisis.	Las prácticas de desarrollo seguro para aplicaciones financieras suelen ser muy rigurosas.

Mitigación: Las estrategias deben enfocarse en proteger los datos en movimiento y asegurar los puntos de transición y transformación:

- Reforzar la Segmentación y el Perímetro: Implementar y mantener una DMZ industrial robusta entre OT e IT, con reglas de firewall estrictas basadas en el principio de mínimo privilegio. Monitorizar el tráfico que cruza este perímetro.

- Cifrado en Tránsito: Utilizar VPNs (IPsec) o TLS/SSL para cifrar las comunicaciones entre la planta, el Edge, los sistemas IT y la nube, siempre que sea posible y compatible con los sistemas OT.

- Hardening de Gateways y Dispositivos Edge: Cambiar credenciales por defecto, deshabilitar servicios innecesarios, aplicar parches de firmware regularmente, restringir el acceso administrativo.

- Prácticas de Codificación Segura para ETL:
    - Validar y sanitizar todas las entradas de datos.
    - Utilizar herramientas de análisis estático de código (SAST) para Python y otros lenguajes.
    - Realizar análisis de composición de software (SCA) para detectar librerías con vulnerabilidades conocidas.
    - Gestionar secretos (credenciales, claves API) de forma segura utilizando bóvedas de secretos o variables de entorno seguras, no embebidos en el código.

- Seguridad de APIs: Implementar autenticación (OAuth 2.0, API Keys), autorización granular, validación de esquemas, cifrado (TLS) y limitación de tasa (rate limiting) para todas las APIs expuestas.

Etapa 3: Almacenamiento y Procesamiento (Infraestructura IT/Cloud)

Descripción de la Etapa y Activos Clave

Una vez transportados y transformados (ETL), los datos industriales llegan a esta etapa donde son almacenados de forma persistente para su uso a corto, mediano y largo plazo. Aquí residen los datos históricos y procesados que alimentarán análisis complejos, modelos de Machine Learning, informes de gestión y cuadros de mando. Esta infraestructura de almacenamiento puede residir on-premise dentro de la red corporativa IT, en la nube, o en un entorno híbrido. Los activos clave incluyen:

- Bases de Datos Relacionales: Como Oracle, SQL Server, PostgreSQL, utilizadas para almacenar datos estructurados, metadatos o resultados de análisis.
- Data Warehouses: Bases de datos optimizadas para consultas analíticas y Business Intelligence, que almacenan datos transformados y agregados.
- Plataformas Cloud: Servicios PaaS/SaaS en la nube que ofrecen capacidades de almacenamiento y procesamiento (ej. AWS IoT, Azure IoT Hub, Google Cloud IoT Platform, servicios de bases de datos gestionadas).

Resultados: Vulnerabilidades y Amenazas Identificadas

Los repositorios de datos centralizados son objetivos atractivos para los atacantes. Las vulnerabilidades comunes incluyen:

- Control de Acceso Débil o Inadecuado: Permisos excesivos otorgados a usuarios o aplicaciones, uso de cuentas genéricas, falta de separación de roles dentro de las bases de datos o plataformas de almacenamiento.
- Configuraciones Inseguras: Bases de datos, servicios cloud o sistemas operativos subyacentes con configuraciones por defecto inseguras (puertos abiertos, servicios innecesarios, auditoría deshabilitada). Específicamente en cloud, errores comunes como buckets de almacenamiento configurados como públicos.

- Vulnerabilidades de Software No Parcheadas: Falta de aplicación de parches de seguridad en el software de gestión de bases de datos o en el sistema operativo host.

- Inyección de Código: Si las aplicaciones que acceden a los datos no validan adecuadamente las entradas, pueden ser vulnerables a ataques de inyección que permitan extraer, modificar o eliminar datos.

- Backups Inseguros o Insuficientes: Copias de seguridad no cifradas, almacenadas en la misma red que los datos primarios, sin pruebas de restauración regulares, o sin copias inmutables/offline.

Las amenazas asociadas a estas vulnerabilidades son significativas: Ransomware, filtración de datos (parámetros de procesos, fórmulas, diseños), manipulación o destrucción de Datos, amenazas internas, explotación de vulnerabilidades de BBDD.

Discusión: Impacto, Análisis Comparativo y Mitigación

El impacto de un incidente de seguridad en esta etapa puede ser severo. La pérdida o corrupción de datos históricos puede impedir análisis de tendencias, optimización de procesos, mantenimiento predictivo y la capacidad de cumplir con auditorías o regulaciones que requieran registros históricos (por ejemplo, informes de consumo energético para ISO 50001). El ransomware puede paralizar no solo el acceso a datos históricos sino potencialmente afectar sistemas que dependen de estas bases de datos para operar, además de la costosa recuperación (si es posible). La exfiltración de datos puede resultar en pérdida de ventaja competitiva o daños reputacionales.

Tabla 3.

Análisis Comparativo (vs. Sector Financiero):

Comparativo	Industria	Finanzas
Impulsores de Seguridad	Si bien protege su propiedad intelectual, a menudo carece de la misma presión regulatoria externa sobre los datos operacionales puros (a menos que se mezclen con PII)	La seguridad del almacenamiento de datos está fuertemente impulsada por regulaciones como GDPR, CCPA, PCI-DSS y normativas bancarias locales. Estas exigen controles estrictos sobre datos personales y financieros, incluyendo cifrado robusto en reposo, enmascaramiento de datos sensibles (Data Masking), controles de acceso muy granulares y pistas de auditoría detalladas e inalterables
Tecnologías y Prácticas	Utilizan tecnologías de bases de datos robustas (como **Oracle**, que ofrece múltiples opciones de seguridad avanzada como TDE, Database Vault, Audit Vault). Sin embargo, no son implementados o implementados de manera incorrecta.	la *implementación* rigurosa de controles como el cifrado en reposo, el enmascaramiento y la auditoría detallada puede ser más consistentemente aplicada en finanzas debido a los requisitos de cumplimiento explícitos. La gestión de identidades y accesos (IAM) para bases de datos también suele ser más madura.
Respuesta a Incidentes	La respuesta puede priorizar la restauración de la disponibilidad de datos para la operación y análisis.	Los planes de respuesta están muy enfocados en la contención de brechas de datos PII y el cumplimiento de notificación a reguladores y clientes

Mitigación: La protección de datos en reposo requiere un enfoque multicapa:

- Hardening de Bases de Datos y Sistemas Operativos: Aplicar guías de configuración segura (ej. CIS Benchmarks), deshabilitar funciones innecesarias, aplicar parches de seguridad regularmente.

- Control de Acceso Estricto (Principio de Mínimo Privilegio): Implementar Role-Based Access Control (RBAC) en bases de datos y plataformas de

almacenamiento. Asegurar que usuarios y aplicaciones solo tengan los permisos estrictamente necesarios. Utilizar autenticación robusta.

- Cifrado en Reposo: Implementar cifrado a nivel de base de datos (ej. Transparent Data Encryption - TDE en Oracle/SQL Server), a nivel de sistema de archivos, o utilizando las capacidades de cifrado de los proveedores de cloud. Cifrar también las copias de seguridad.

- Seguridad de la Configuración Cloud: Utilizar herramientas de Cloud Security Posture Management (CSPM) para detectar y remediar configuraciones inseguras en servicios de almacenamiento cloud (buckets, bases de datos gestionadas). Implementar políticas de acceso IAM granulares en la nube.

- Protección contra Inyecciones: Asegurar que las aplicaciones que interactúan con las bases de datos utilicen consultas parametrizadas (prepared statements) y validen/saniticen todas las entradas. Utilizar Web Application Firewalls (WAFs) si el acceso es vía web.

- Estrategia de Backup y Recuperación Robusta: Implementar la regla 3-2-1 (tres copias, dos medios diferentes, una offline/offsite). Asegurar que los backups estén cifrados y, crucialmente, considerar backups inmutables (WORM - Write Once, Read Many) para proteger contra ransomware. Realizar pruebas de restauración periódicas.

- Monitorización y Auditoría: Habilitar y revisar regularmente los logs de auditoría de las bases de datos y sistemas de almacenamiento. Utilizar herramientas de Database Activity Monitoring (DAM) para detectar actividades sospechosas en tiempo real.

Etapa 4: Análisis, Visualización y Acción (Plataformas BI/Aplicaciones)

Descripción de la Etapa y Activos Clave

Esta es la etapa final del ciclo de vida del dato industrial, donde la información almacenada y procesada se transforma en conocimiento accionable y se presenta a los usuarios para la toma de decisiones, monitorización o incluso para desencadenar acciones automatizadas. Es la interfaz entre los datos complejos y los usuarios de negocio, ingenieros, analistas u operadores. Los activos clave en esta fase son diversos e incluyen:

- Plataformas de Business Intelligence (BI): Herramientas como Power BI o específicas de dominio como GridVis, que permiten crear informes interactivos, cuadros de mando y visualizaciones.

- Herramientas y Entornos de Análisis Avanzado: Incluyen lenguajes como Python o R, utilizados en notebooks (Jupyter) o entornos de desarrollo para realizar análisis estadísticos, modelado predictivo y análisis exploratorio.

- Plataformas Low-Code/No-Code: Como Microsoft Power Platform, que permiten a usuarios con menos conocimientos de programación crear aplicaciones de negocio y flujos de trabajo automatizados que consumen y, a veces, modifican datos.

- Plataformas de Colaboración y Gestión Documental: Como SharePoint, utilizadas para compartir informes, datasets, documentación y colaborar en análisis.

Resultados: Vulnerabilidades y Amenazas Identificadas

Incluso si los datos se han protegido en las etapas anteriores, la capa de consumo introduce sus propios riesgos:

- Gestión de Permisos Inadecuada: Configuración incorrecta de permisos en plataformas BI, sitios de SharePoint, o aplicaciones Power Platform, otorgando acceso excesivo a datos o funcionalidades sensibles a usuarios no autorizados.

- Vulnerabilidades en Código de Análisis/Modelos: Errores o vulnerabilidades en el código Python utilizado para análisis o modelos de ML (ej. librerías inseguras, lógica defectuosa que puede ser explotada).

- Desarrollo Inseguro en Plataformas Low-Code: Aplicaciones Power Platform sin formación en seguridad, que pueden tener lógica defectuosa, conectores inseguros, permisos mal gestionados o exponer datos sensibles inadvertidamente.

- Compartición Insegura de Informes/Datos: Exportación de datos sensibles desde plataformas BI a formatos inseguros (Excel, CSV) y compartición por canales no controlados (email, etc.). Publicación de informes en espacios públicos o con audiencias demasiado amplias.

- Ataques del Lado del Cliente: Si las herramientas son basadas en web, pueden ser susceptibles a ataques como Cross-Site Scripting (XSS) si la plataforma tiene vulnerabilidades, o ataques de phishing dirigidos a los usuarios para robar credenciales de acceso a estas plataformas.

Las amenazas en esta fase incluyen: fuga de información confidencial, acceso no autorizado a insights, phishing y robo de Credenciales, explotación de aplicaciones Low-Code

Discusión: Impacto, Análisis Comparativo y Mitigación

El impacto de una brecha de seguridad en la capa de consumo puede ser significativo, aunque a menudo menos directo que un ataque a la capa OT. La fuga de

información sobre eficiencias de producción, consumo energético detallado (ISO 50001), o planes de mantenimiento puede erosionar la ventaja competitiva. El acceso no autorizado a análisis predictivos o estratégicos puede tener implicaciones financieras o de mercado. Decisiones basadas en informes comprometidos o el mal funcionamiento de aplicaciones low-code críticas pueden llevar a errores operativos o de negocio. Además, pueden surgir problemas de cumplimiento si datos que puedan considerarse sensibles son expuestos indebidamente.

Tabla 4.

Análisis Comparativo (vs. Sector Financiero):

Comparativo	Industria	Finanzas
Seguridad de Aplicaciones Internas	El auge de plataformas low-code como **Power Platform** en todos los sectores introduce el desafío de asegurar aplicaciones creadas por usuarios no expertos en seguridad, un reto quizás más novedoso o extendido que en los desarrollos Java tradicionales de banca.	Las aplicaciones internas en finanzas (ej. para análisis de riesgo, detección de fraude) suelen pasar por procesos de desarrollo seguro y auditorías rigurosas
Auditoría y Monitorización	Herramientas como **Power BI** y **SharePoint** ofrecen capacidades de auditoría, pero su configuración y revisión activa pueden no ser tan prioritarias en todos los entornos industriales	La capacidad de auditar quién accedió a qué informe o dato es crucial en finanzas para el cumplimiento

Mitigación: Asegurar la capa de consumo requiere un fuerte enfoque en la gobernanza del acceso y la seguridad de las aplicaciones:

- Gestión Rigurosa de Permisos: Implementar el principio de mínimo privilegio en todas las plataformas (Power BI, SharePoint, Power Platform). Utilizar grupos de seguridad, roles y compartir contenido de forma controlada (evitar compartir con "Todos").

- Gobernanza de Power Platform: Establecer una estrategia de entornos (separar desarrollo, pruebas, producción), aplicar políticas de Prevención de Pérdida de Datos (DLP) para controlar qué conectores se pueden usar juntos, monitorizar el uso de conectores personalizados y premium.

- Prácticas Seguras de Desarrollo (Analytics & Low-Code): Aplicar principios de codificación segura a scripts Python de análisis. Establecer directrices y revisiones para aplicaciones Power Platform críticas.

- Seguridad de Endpoints y Navegadores: Asegurar los dispositivos desde los cuales los usuarios acceden a estas plataformas.

- Concienciación y Formación del Usuario: Educar a los usuarios sobre los riesgos de compartir información, phishing, y el uso seguro de las herramientas de BI y colaboración.

- Data Loss Prevention (DLP): Implementar soluciones DLP a nivel de endpoint, red o cloud para detectar e impedir la exfiltración de datos sensibles.

Conclusiones

Este estudio ha analizado de manera integral los desafíos de ciberseguridad inherentes al ciclo de vida completo de los datos en el contexto de la Industria 4.0, desde su generación en la planta hasta su consumo en aplicaciones analíticas y de negocio. La investigación confirma que los riesgos son significativos y permean cada etapa: desde la vulnerabilidad de los sistemas OT legados y protocolos inseguros en la capa de control (Etapa 1), pasando por los peligros de intercepción o manipulación durante el transporte y la transformación ETL (Etapa 2), los riesgos de brecha, pérdida o ransomware sobre los datos almacenados (Etapa 3), hasta la potencial fuga de información o el acceso no autorizado a través de las herramientas de análisis y visualización (Etapa 4).

El análisis comparativo con el sector financiero ha sido instrumental para resaltar la singularidad del desafío industrial. Las diferencias fundamentales en las prioridades de seguridad (Disponibilidad y Seguridad Operacional vs. Confidencialidad e Integridad), los entornos tecnológicos, los impulsores regulatorios y la tolerancia al riesgo operativo dictan que un enfoque de "copiar y pegar" las estrategias de seguridad IT/financiera es inadecuado y potencialmente contraproducente para la Industria 4.0. Si bien se pueden extraer lecciones valiosas del sector financiero en áreas como la madurez de la gestión de riesgos o las prácticas de desarrollo seguro, estas deben ser cuidadosamente adaptadas al contexto industrial.

La conclusión fundamental es que asegurar la Industria 4.0 requiere un enfoque holístico, basado en el riesgo, y profundamente contextualizado, que considere la seguridad de manera integral a lo largo de todo el ciclo de vida del dato. La protección no puede centrarse únicamente en el perímetro IT/OT o en componentes aislados, sino que debe abarcar desde el sensor hasta la nube y las aplicaciones finales.

Es importante reconocer las limitaciones inherentes a este estudio. Su naturaleza es principalmente cualitativa y analítica, basada en la revisión de literatura, estándares y la síntesis de conocimiento experto, y no incluye validación empírica mediante pruebas de penetración o recolección de datos cuantitativos primarios sobre incidentes o efectividad de controles. Las generalizaciones realizadas sobre los entornos industriales y financieros pueden no aplicarse uniformemente a todas las organizaciones específicas dentro de esos sectores, dada la gran variabilidad existente. Finalmente, aunque informado por experiencia profesional, el análisis se basa en interpretaciones y síntesis, no en la divulgación de datos específicos o confidenciales de ninguna organización en particular.

Los hallazgos y limitaciones de este estudio abren diversas vías para futuras investigaciones y desarrollos en el campo de la ciberseguridad para la Industria 4.0:

- Análisis Cuantitativos: Realizar estudios que cuantifiquen el impacto real de ciberataques específicos en diferentes subsectores industriales o que midan la efectividad (y el retorno de inversión) de controles de seguridad específicos para OT.

- Seguridad de Tecnologías Emergentes: Investigar en profundidad los riesgos y controles de seguridad asociados a tecnologías clave de Industria 4.0 como la Inteligencia Artificial y el Machine Learning aplicados a procesos industriales.

- Factor Humano en OT: Profundizar en el estudio del comportamiento humano, la concienciación situacional y el desarrollo de programas de formación en ciberseguridad efectivos y adaptados específicamente para ingenieros, técnicos y operadores de planta.

- Automatización de la Seguridad OT: Investigar y desarrollar herramientas y técnicas para la monitorización, detección de amenazas y respuesta automatizada que sean seguras y efectivas en entornos OT en tiempo real.

- Seguridad de la Cadena de Suministro Industrial: Analizar los riesgos introducidos por terceros y desarrollar marcos para gestionar la seguridad de la cadena de suministro OT.

- Seguridad de Plataformas Low-Code en Industria: Dada la creciente adopción de plataformas como Microsoft Power Platform para crear aplicaciones que interactúan con datos y procesos industriales, se necesita investigación específica sobre las mejores prácticas, modelos de gobernanza y controles técnicos para asegurar estas aplicaciones en contextos potencialmente críticos.

Referencias bibliográficas

International Society of Automation & International Electrotechnical Commission. (2018). Security for industrial automation and control systems: Technical security requirements for IACS components. (ANSI/ISA-62443-4-2-2018). https://www.isa.org/products/ansi-isa-62443-4-2-2018-security-for-industrial-au.

International Organization for Standardization & International Electrotechnical Commission. (2022). Information security, cybersecurity and privacy protection - Information security management systems – Requirements. (ISO/IEC 27001:2022). https://www.iso.org/standard/27001

International Organization for Standardization. (2013). Financial services -Universal financial industry message scheme - Part 6: Message transport characteristics. (ISO 20022-6:2013).

https://www.iso.org/standard/61102.html

International Organization for Standardization. (2018). Energy management systems - Requirements with guidance for use. (ISO 50001:2018). https://www.iso.org/standard/69426.html

National Institute of Standards and Technology. (2024). Framework for improving critical infrastructure cybersecurity, version 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Escaño González, J. M. (2025). Ciberseguridad industrial. Editorial Académica. https://books.google.com.ec/books?id=EbZSEQAAQBAJ

Belmar Muñoz, V. (2024). El principio de Pareto o criterio 80-20 en la empresa. Academia. https://www.academia.edu/122608372/EL_PRINCIPIO_DE_PARETO_O_CRITERIO_80_20

Andrango Alobuela, M. S., & Arroyo Morocho, F. R. (2022). Industria 4.0 y economía circular: Revisión de la literatura y recomendaciones para una industria sustentable en Ecuador. Ciencia Latina Revista Científica Multidisciplinar. https://ciencialatina.org/index.php/cienciala/article/view/1422/1966

ISA Global Cybersecurity Alliance (ISAGCA). (2020). ISAGCA Quick Start Guide. https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf

Ghelani, D., Tan, K. H., & Koduru, S. K. R. (2022). Cyber security threats, vulnerabilities, and security solutions models in banking. American Journal of Computer Science and Technology. https://www.authorea.com/doi/full/10.22541/au.166385206.63311335

Belman-López, C. E., Jiménez-García, J. A., Vázquez-López, J. A., & Camarillo-Gómez, K. A. (2023). Diseño de una arquitectura para sistemas y aplicaciones en Industria 4.0 basada en computación en la nube y análisis de datos. Revista Iberoamericana de Automática e Informática Industrial, 137-149. https://doi.org/10.4995/riai.2023.17791

García Núñez, N. (2023). Análisis, explotación y refuerzo de vulnerabilidades en entornos de convergencia IT/OT. Repositorio UVaDoc. https://uvadoc.uva.es/bitstream/handle/10324/71360/TFG-G6914.pdf

López Prieto, L. C., Moreno, D. A., Moreno Chingaté, D. A., & Serrato Rodríguez, Y. I. (2022). Adopción de buenas prácticas en seguridad de la información enfocado en ambientes. Repositorio Institucional Los Libertadores. https://repository.libertadores.edu.co/server/api/core/bitstreams/36228d25-439b-4540-aaf5-9b9c82432592/content.