REVISTA FORMACIÓN ESTRATÉGICAISSN 2805-9832
Vol. 10 Núm. 2 (2024)
Recibido agosto 2024 –Aceptado enero 2025

Seguridad Informática en la Industria Moderna, un enjambre de retos y estadísticas

Cybersecurity in the Modern Industry, a swarm of challenges and statistics

PhD. Francisco Raúl Arencibia-Pardo
francisco.arencibia@unipamplona.edu.co
https://orcid.org/0000-0001-6012-2577
Facultad de Ingenierías y arquitectura
Programa Maestría en Ingeniería Industrial
Universidad de Pamplona, Colombia

Msc. Belisario Peña-Rodríguez
belisariop@unipamplona.edu.co
https://orcid.org/0000-0001-9859-7658
Facultad de Ingenierías y arquitectura
Programa de Ingeniería Industrial
Universidad de Pamplona, Colombia

Correspondencia: **PhD. Francisco Raúl Arencibia-Pardo** Magister en Educación https://orcid.org/0000-0001-6012-2577 Programa Maestría en Ingeniería Industrial, Universidad de Pamplona, Colombia
.

RESUMEN

Es un hecho; los temas sobre seguridad informática, se han convertido en la base de los logros, la eficiencia y la operatividad de la industria actual. El presente trabajo de revisión, transita por la evolución de la seguridad informática, las amenazas a que se enfrentan los emprendimientos, las estrategias de protección y mitigación implementadas, así como el estudio de casos de ataques cibernéticos que han hecho tambalear la industria. Para lograr los objetivos propuestos, se realizó una investigación fundamentada y métodos de revisión basados en la analítica que aportaron decenas de publicaciones con alto rigor científico, informes competentes, así como la exploración de las normas relacionadas con la ciberseguridad técnica.
Se hizo uso de las normativas APA 7ma edición para la cita y referenciación de más de 30 fuentes especializadas. El análisis resultante seccionó los sectores metalúrgicos, energía, salud y transporte, recalcando la jerarquía de una infraestructura cibernética actual y segura.

Palabras clave: Ciberseguridad industrial, Infraestructura crítica, Ransomware, Defensa en profundidad, Industria 4.0.

REVISTA FORMACIÓN ESTRATÉGICAISSN 2805-9832
Vol. 10 Núm. 2 (2024)
Recibido agosto 2024 –Aceptado enero 2025

ABSTRACT

It is a fact; topics related to cybersecurity have become the foundation for achievements, efficiency, and operability in today's industry. This review paper traces the evolution of cybersecurity, the threats faced by businesses, the protection and mitigation strategies implemented, as well as case studies of cyber-attacks that have shaken the industry. To achieve the proposed objectives, a grounded investigation and review methods based on analytics were conducted that provided dozens of publications with high scientific rigor, competent reports, as well as an exploration of the regulations related to technical cybersecurity.
The APA 7th edition guidelines were used for citing and referencing more than 30 specialized sources. The resulting analysis segmented the metallurgy, energy, health, and transportation sectors, emphasizing the hierarchy of a current and secure cyber infrastructure.

Keywords: Industrial cybersecurity, Critical infrastructure, Ransomware, Defense in depth, Industry 4.0.

RESUMO

É um fato; os temas sobre segurança informática tornaram-se a base dos sucessos, da eficiência e da operatividade da indústria atual. Este trabalho de revisão aborda a evolução da segurança informática, as ameaças enfrentadas pelas empresas, as estratégias de proteção e mitigação implementadas, bem como o estudo de casos de ataques cibernéticos que abalaram a indústria. Para alcançar os objetivos propostos, foi realizada uma investigação fundamentada e métodos de revisão baseados na análise que forneceram dezenas de publicações com alto rigor científico, relatórios competentes, assim como a exploração das normas relacionadas com a cibersegurança técnica.
Foi utilizada a normatização APA 7ª edição para a citação e referenciação de mais de 30 fontes especializadas. A análise resultante seccionou os setores metalúrgico, energético, saúde e transporte, sublinhando a hierarquia de uma infraestrutura cibernética atual e segura.

Palavras-chave: Cibersegurança industrial, Infraestrutura crítica, Ransomware, Defesa em profundidade, Indústria 4.0.

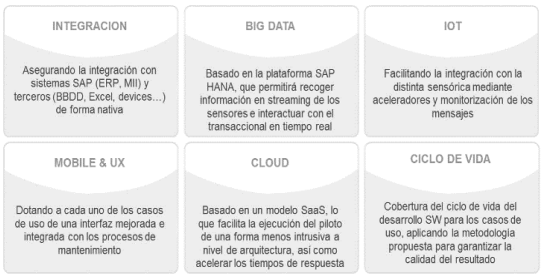
Introducción

Si de algo no puede hablarse en la fabricación moderna, es sobre rutina. A partir del siglo XX, La industria ha transformado profundamente su dinámica, para poder dar respuesta a los desafíos de una época marcada por cambios abruptos (Nordström et al., 2006).
La transformación de la seguridad informática en los procesos productivos también ha evolucionado y se ha dinamizado. Lejos quedan los 80, cuando la protección se limitaba a los accesos y mediante guardias. Al ser casi nula la conectividad, redactan Royakkers et al., (2018), los riesgos eran casi inexistentes, como también la capacidad de respuesta.

REVISTA FORMACIÓN ESTRATÉGICAISSN 2805-9832
Vol. 10 Núm. 2 (2024)
Recibido agosto 2024 –Aceptado enero 2025

En los 90 comenzó la era de la internet y con ella, surgieron nuevas amenazas a la seguridad. Los firewalls y los antivirus, destacan Landauer et al., (2024), aunque eficaces, comenzaron a quedarse obsoletos ante los ciberataques.
Arribó la revolución 4,0, la inteligencia artificial y el big data, entre otros desafíos totalmente disruptivos del siglo XXI. La conectividad ininterrumpida y los datos viajando por la nube, incrementaron abruptamente la sed por ataques a la seguridad informática (Malatji & Tolah, 2025).
La digitalización de los procesos industriales, por tanto, ha dado un vuelco notable a las organizaciones. Puede decirse que, hoy en día, los mismos operan con dependencia [en aumento] de sistemas informáticos que se encuentran interconectados (Fernández, M. Á., & Pajares, R. 2017).
Sin embargo, esta transformación también ha incrementado la exposición a riesgos cibernéticos. La razón es simple: ha dejado de ser un problema técnico para transformarse en una razón de índole estratégica, afectando la continuidad del negocio, la reputación empresarial y, por ende, la confianza del cliente.

TABLA 1. Incorporación de la digitalización a la industria



Las empresas han creado dependencia de tecnologías interconectadas para su funcionamiento diario, por tanto, como refiere Atlantic International University (2024), la ciberseguridad es hoy un pilar esencial en la garantía de la continuidad del negocio, marcado por un entorno digital cada vez más retador.
Son muchas las empresas o las ramas productivas sometidas al embate de la modernidad. Impulsadas por la necesidad de reducir costos, minimizar el impacto ambiental y acomodar sus producciones a las exigencias verdes, pueden ver afectada la confianza del consumidor en un panorama donde, tanto los datos personales como empresariales, circulan tenazmente.

Actualmente, los clientes no solo esperan productos y servicios de calidad, sino también sentir la tranquilidad de que sus datos son protegidos. Invertir en seguridad informática, por tanto, no solo es una medida preventiva, sino apostar por la sostenibilidad y la competitividad a largo plazo.

La digitalización en la industria beneficia enormemente al sector empresarial, pero también ha incrementado su responsabilidad. Colocar tecnologías avanzadas sin una estrategia de ciberseguridad al final será contraproducente. La clave está, aconseja Westerman (2025), en comprender que la transformación digital no es solamente ser eficiente, sino también

transmitir confianza, resiliencia y visión estratégica, mediante una comprensión realista de los riesgos que se encuentra sometida la manufactura y sus vías de solución.

Método

La presente investigación busca percibir la defensa de los activos digitales en diferentes contextos organizacionales. Se consideran los riesgos a qué se enfrentan, así como las estrategias implementadas para su mitigación.

Diseño metodológico empleado.

Se adopta un método mixto, combinando enfoques cuantitativos y cualitativos. Mediante esta selección, se analizan datos estadísticos como experiencias de las empresas seleccionadas y sus sectores.

Se escogen como muestra representativa, los siguientes sectores empresariales:

1. Industria de materiales de construcción.
2. Educación Superior.
3. La industria del software.
4. La industria del petróleo.
5. Industria cafetalera.
6.

Enfoque cuantitativo:

Se aplicarán encuestas estructuradas, según Del Canto (2013). Estas encuestas permitirán medir variables como el nivel de madurez en ciberseguridad, la frecuencia de incidentes, el tiempo de respuesta y la inversión en protección digital. Los datos serán analizados mediante estadística descriptiva y comparativa para identificar patrones y diferencias entre industrias.

Enfoque cualitativo:

Entrevistas semiestructuradas y análisis de documentos [artículos, documentos institucionales, políticas de seguridad y marcos normativos]. Con este enfoque expondremos los desafíos específicos que enfrenta cada industria escogida, las estrategias adoptadas y la cultura organizacional sobre la ciberseguridad.

Este enfoque metodológico permitirá no solo describir el estado actual de la seguridad digital en diferentes sectores industriales, sino también identificar problemas de seguridad y oportunidades de mejora. Así, se espera contribuir a una comprensión más profunda y estratégica de la ciberseguridad como un factor clave para la sostenibilidad organizacional en la era digital.

La industria de materiales de construcción. Riesgos y ciberseguridad; nuevo desafío.

Fabricar el acero y el cemento, conlleva a peligrosas emisiones de CO_2 a la atmósfera. Para minimizar su impacto ambiental, se están desarrollando e implementando materiales alternativos como son el concreto con retención de carbono, bioconcreto, ladrillos hechos de materiales reciclados, combinados con el cáñamo industrial.

En el apartado de software, se trabaja con BIM para el modelaje y la impresión 3D. En los materiales constructivos, la innovación ha recabado entre sus principales logros, el de la sostenibilidad. La mejora de la calidad de vida mediante la relación del adobe en el

perfeccionamiento de las propiedades estructurales, narran (Álvarez & Ospino, 2020), son un punto extra en el aumento de la calidad de vida de los inquilinos.

A medida que la industria de materiales para la construcción se desarrolla y diseña una gama de nuevos productos, el know-how digital comienza a integrarse. Entonces aparecen los riesgos ante los ataques informáticos y la vulnerabilidad en la red, ocurriendo robos o modificación de las innovaciones, hackeo de los sensores y arremetidas a la cadena de suministro, apoderándose tanto del software como del hardware (Márquez Díaz et al., 2024).

La Educación Superior 4.0. Novedosas plataformas, desconocidos peligros.

Los estudios superiores no son ajenos a la influencia de las tecnologías de la Industria 4.0. Las mismas, afirman (Carrero et al., 2022), abren nuevas posibilidades para las aplicaciones y los servicios académicos. Si hablamos de educación 4.0 e ingenieros 4.0, debemos pasar por las innovaciones para el terreno de la educación superior, exponencialmente incrementadas durante el Covid 19.

Las tecnologías digitales integradas al entorno educativo es un hecho, al igual que el aumento de la inseguridad, expresa (Muñoz, 2024), por tanto, no puede existir educación moderna sin la ciberseguridad. Manejar la Educación 4.0 conlleva un entorno de inviolabilidad de la información de los estudiantes, los docentes y el personal administrativo.
Los entornos educativos digitales enfrentan diversos riesgos de ciberseguridad, entre los cuales se destacan el robo de los datos, suplantación de la identidad, hackeo de las plataformas educativas, phishing y malware. Una descripción de los mismos sería:

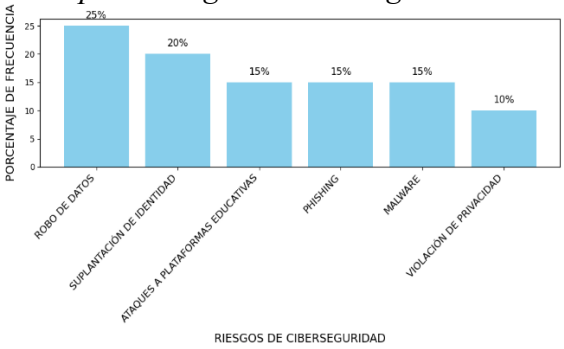
TABLA 2. Descripción de los principales riesgos

PRINCIPALES RIESGOS	DESCRIPCIÓN
ROBO DE DATOS	ACCIONES MALICIOSAS PARA OBTENER INFORMACIÓN CONFIDENCIAL
SUPLANTACIÓN DE IDENTIDAD	USO NO AUTORIZADO DE IDENTIDADES PARA ACCEDER A RECURSOS
ATAQUES A PLATAFORMAS EDUCATIVAS	INTENTOS DE INTERRUPCIÓN O CONTROL DE SISTEMAS EDUCATIVOS
VULNERABILIDADES EN SOFTWARE	FALLAS EN PROGRAMAS QUE PUEDEN SER EXPLOTADAS POR ATACANTES

El porcentaje de frecuencia de aparición de estos en el entorno educativo, podemos apreciarlo en la figura 1.

REVISTA FORMACIÓN ESTRATÉGICAISSN 2805-9832
Vol. 10 Núm. 2 (2024)
Recibido agosto 2024 –Aceptado enero 2025

Figura 1:
Principales riesgos de ciberseguridad en entornos educativos digitales.



La industria del software, a manera de proyecto de inversión, tampoco se libra del riesgo.

Son muchos los equipos de ingeniería y diseño de procedimientos, que trabajan en el desarrollo de aplicaciones para la industria del software. Planteado como un proyecto de inversión (o parte del mismo), apoyo al PMI o inculcando potencia a los entregables en una inversión (Puentes et al., 2022), parecería una gran idea, siempre y cuando comprendamos que, nos guste o no, nos encontramos en una peligrosa situación de riesgos sobre seguridad informática.

Al colocarnos como desarrolladores de software, rara vez asumimos que nuestro resultado no sea precisamente funcional, mucho menos seguro. Es un error pensar así, ya que, sin querer, estamos complicando la probidad del producto, la confianza de nuestro cliente potencial y, lo peor, la factibilidad.
Dentro de los aspectos a tener en cuenta si deseamos seguridad de la información, son los errores en que se incurren durante la programación, los que pueden ser utilizados, tanto para extraer datos como introducir ransomware o phishing. Igualmente, pueden existir malas practica internas con huella directa en la reputación de la empresa.
En el mundo actual, los países protegen el software y sus aplicaciones. Para ello deben seguir una serie de regulaciones sobre cómo salvaguardar tus datos.
TABLA 2. Comparación de reglamentos a nivel mundial.

Nombre del Reglamento	**País o Región**	**Entrada en Vigor**	**Descripción Breve**
RGPD (Reglamento General de Protección de Datos)	Unión Europea	2018	Marco integral para la protección de datos propios en la UE.

Nombre del Reglamento	País o Región	Entrada en Vigor	Descripción Breve
CCPA (California Consumer Privacy Act)	California, EE. UU.	2020	Otorga a los consumidores derechos sobre sus datos personales y su mercadeo.
LGPD (Lei Geral de Proteção de Dados)	Brasil	2020	Regula el tratamiento de datos íntimos en Brasil.
PIPEDA (Personal Information Protection and Electronic Documents Act)	Canadá	2000 (actualizada)	Regula cómo las empresas privadas manejan los datos personales.
APPI (Act on the Protection of Personal Information)	Japón	2005 (revisada en 2022)	Normas para el uso de datos personales por entidades privadas.
PDPA (Personal Data Protection Act)	Singapur	2012	Equilibra la protección de datos con la necesidad de innovación empresarial.
DPA (Digital Personal Data Protection Act)	India	2023	Regula el uso de datos propios y otorga derechos a los ciudadanos.
POPIA (Protection of Personal Information Act)	Sudáfrica	2021	Protege datos personales y regula su procesamiento.

Nombre del Reglamento	País o Región	Entrada en Vigor	Descripción Breve
Privacy Act	Australia	1988 (revisada)	Regula el manejo de información por agencias gubernamentales y empresas.

Entre estos tenemos:

Reglamento General de Protección de Datos de la Unión Europea. Este estatuto, conocido también como Reglamento (UE) 2016/679, es una normativa de la Unión Europea en vigor desde el 2018. Su objetivo principal radica en la protección de los datos personales y la libre circulación europea (EUR-LEX, 2022).

La ley pretende unificar la protección de datos en la Unión, facilitando el comercio digital y la innovación. Además, se nutre de los derechos al acceso, a la corrección de datos, eliminación de los datos que no se usan, transferencia de los mismos, negarse a su tratamiento (no siempre), a la transparencia y otros.

En los Estados Unidos se posee, para ejemplificar, a la Ley de Privacidad del Consumidor de California. La misma va dirigida a los empresarios que utilizan datos de residentes (Drmunozcl, 2025).

El pleno derecho del comprador a conocer cuales datos sobre su persona se compilan, a solicitar cuando desee que estos sean eliminados, escoger no compartirlos, son varios de los lineamientos que acumula esta ley.

Petróleo, extracción, modernidad y riesgos.

Múltiples son las especialidades que colaboran en el mundo petrolero. De ellos, gran parte se concentra en la extracción y los sofisticados medios para lograrlo.

Una de las propuestas investigadas, va dirigida a las fallas en lo concerniente a los pozos de extracción. Mediante un producto mecatrónico de alta complejidad (SmartOMP), podemos identificar con exactitud y premura las fallas de un pozo, controlando el riesgo operacional e influyendo en los niveles de producción (Flórez & Salazar, 2020), incorporando un sistema automático inteligente que reconoce patrones de falla en el bombeo mecánico.

SmartOMP trabaja en tiempo real. Lee el dinagrama del fondo de pozo, utilizando un sistema en la cabeza de pozo y otro colocado a distancia. Parecería una buena idea, pero carece del componente de seguridad, lo que lo hace un producto vulnerable.

Veamos algunos ejemplos de hackeo a la seguridad informática en el petróleo:

La más grande tubería de productos refinados de los Estados Unidos, Colonial Pipeline, fue atacada por un ransomware en el 2021. Luego de desembolsar 4,4 millones en rescates, quedó en evidencia el sistema informático por el acceso sin autorización mediante credenciales comprometidas, cerrando la planta transitoriamente (Forbes, 2021).

El virus Shamoon atacó 30,000 oficinas de trabajo de la petrolera Saudi Aramco (Perlroth, 2012), impactando en una masiva pérdida de datos y aniquilando las operaciones de la

administración empresarial. Un poderoso malware sobrescribía datos, invalidando los procedimientos
Paralizaciones en las operaciones de PEMEX debido a un ataque del Ransomware, concluyó en la afectación de su labor petrolera. El hecho ocurrió en el 2019 y obligó a laborar en hojas de papel.
Una gran explosión sacudió el Golfo de México en 2010. Errores de los operarios y un software mal configurado que trajo deslices en la interpretación de los datos, causaron 11 muertos y un desastre medioambiental de magnitudes catastróficas. No todo ocurre por ataques cibernéticos, tal y como pudo comprobar la plataforma petrolera Deepwater Horizon (Rodrigo, 2020). La seguridad informática debe estar siempre atenta.

Figura 2:
Derrame de petróleo de Deep Horizon en 2010.

Estos ejemplos nos muestran las consecuencias de un mal manejo de software o la falta de seguridad cibernética. Muertes, secuelas financieras y fatales consecuencias medioambientales, priorizan el protagonismo de la ciberseguridad.

La industria moderna del café colombiano, entra de lleno en las redes neuronales artificiales. Los peligros de hackeo se palpan.

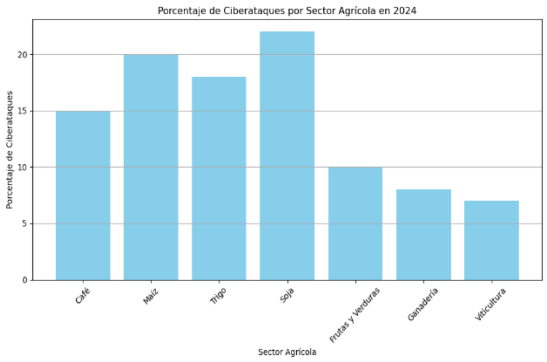
Deleitarse con una buena taza de café colombiano ha dejado de ser una moda internacional, para convertirse en costumbre y, por tanto, la demanda sube y sube. De entre todos los tipos de granos exportables, no dejan de aparecer buenas noticias para el café arábica colombiano de alta calidad.
En el primer trimestre del 2025, el precio de venta a nivel internacional subió de 351.93 centavos de dólar por libra, hasta 394.14, cierre abril. Las exportaciones aumentaron en 1,3% en comparación al 2024, lo que representa un incremento de 01 millones de sacos de arábica suave (Cafetero, 2025). Nada mal.
Para mantener este ritmo de ventas, se necesitan estrictos y estandarizados controles informáticos, no tan solo para el control de la calidad, sino también para lograr establecer predicciones en los precios y realizar mejores negocios.
Una de las investigaciones realizadas en terreno, explica (Rueda, 2022), consiste en aprovechar la capacidad de las redes neuronales artificiales para realizar pronósticos con modelos no lineales para pronosticar y controlar los precios del café de tipo arábico. Los

resultados obtenidos, demuestran la validez de este modelo y su ejercicio en el aprendizaje para minimizar errores a la hora de vender.
Sin embargo, no tener en cuenta los riesgos es un problema, y muy serio. Por citar un ejemplo, en 2021 Jacobs Douwe Egberts, una de las mayores compañías de café del mundo con sede en Ámsterdam, recibió un ciberataque. Aunque la información se trató de mantener en un perfil bajo, sus operaciones tuvieron que ser suspendidas, con las consiguientes pérdidas en la producción y las ventas.

TABLA 3. Tipos de ataques cibernéticos a la agricultura en 2024.

Sector Agrícola	**Tipo de Ciberataque**	**Consecuencias Reportadas**
Café	Ransomware	Interrupción de operaciones y pérdida de datos
Maíz	Phishing	Acceso no autorizado a sistemas financieros
Trigo	Malware	Interrupción de maquinaria agrícola
Soja	Robo de Datos	Robo de propiedad intelectual
Frutas y Verduras	Secuestro de Datos	Encriptación de datos críticos
Ganadería	Ataques a Sistemas de Control	Interrupción de operaciones y daños físicos a equipos
Viticultura	Interrupción de la Cadena de Suministro	Retrasos en la entrega de productos

Figura 2:
Porcentaje de ataques cibernéticos por sector agrícola. Año 2024.



REVISTA FORMACIÓN ESTRATÉGICAISSN 2805-9832
Vol. 10 Núm. 2 (2024)
Recibido agosto 2024 –Aceptado enero 2025

Análisis cuantitativo

Realizando un análisis de tipo estadístico descriptivo, cita Flores (2025), y examinando las variables combinaciones para la ciberseguridad en las cinco industrias relacionadas, obtenemos el siguiente resumen.

TABLA 4. Nivel de madurez (Escala ponderada del 1 al 5).

INDUSTRIA	MEDIA	MEDIANA	DESVIACIÓN ESTÁNDAR
MATERIALES DE CONSTRUCCIÓN	3.08	3.18	0.46
EDUCACIÓN SUPERIOR	3.1	3.15	0.57
SOFTWARE	3.48	3.43	0.55
PETRÓLEO	2.87	2.82	0.42
CAFETALERA	2.76	2.75	0.28

TABLA 5. Frecuencia pon que se desatan los incidentes (Frecuencia anual).

INDUSTRIA	MEDIA	MEDIANA	DESVIACIÓN ESTÁNDAR
MATERIALES DE CONSTRUCCIÓN	4.17	4.0	2.41
EDUCACIÓN SUPERIOR	5.6	5.0	2.81
SOFTWARE	2.87	3.0	1.25
PETRÓLEO	5.0	5.0	2.02
CAFETALERA	3.73	3.5	2.24

TABLA 6. Tiempo de respuesta ante los incidentes (En horas).

INDUSTRIA	MEDIA	MEDIANA	DESVIACIÓN ESTÁNDAR
MATERIALES DE CONSTRUCCIÓN	23.26	23.68	3.8
EDUCACIÓN SUPERIOR	23.56	22.9	4.45
SOFTWARE	12.8	13.12	3.23
PETRÓLEO	27.03	27.44	3.81
CAFETALERA	24.87	25.49	3.97

TABLA 7. Inversión en ciberseguridad (En decenas de miles de USD).

INDUSTRIA	INVERSIÓN PROMEDIO (Decenas de miles USD)
MATERIALES DE CONSTRUCCIÓN	$49,219.00
EDUCACIÓN SUPERIOR	$52,384.46
SOFTWARE	$49,505.77
PETRÓLEO	$103,141.44
INDUSTRIA CAFETALERA	$49,965.39

REVISTA FORMACIÓN ESTRATÉGICAISSN 2805-9832
Vol. 10 Núm. 2 (2024)
Recibido agosto 2024 –Aceptado enero 2025

Para visualizar las variables, utilizaremos el diagrama de caja (Boxplot). Con el podemos representar tanto la dispersión como la simetría de los datos obtenidos por cada una de las industrias, utilizando una sola grafica que refleja de forma clara, simple y compacto los resultados (Estadística, 2021).

Figura 3:
Gráfico de caja del nivel de madurez (2025).

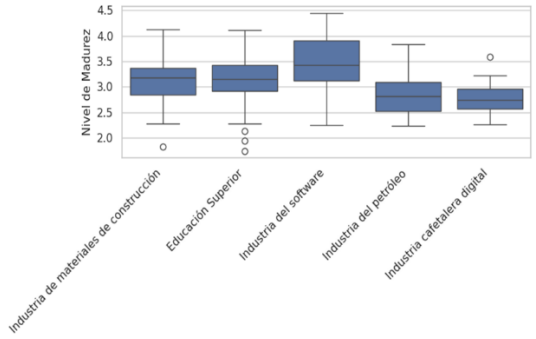


Figura 4:
Gráfico de caja del nivel de incidencias anual (2025).

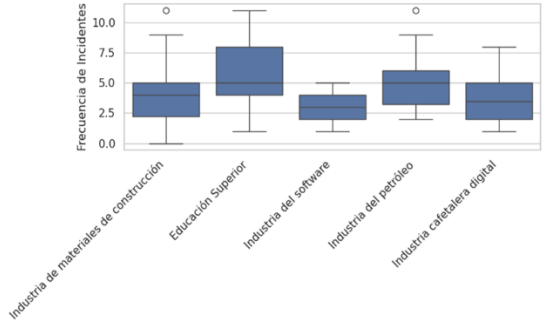
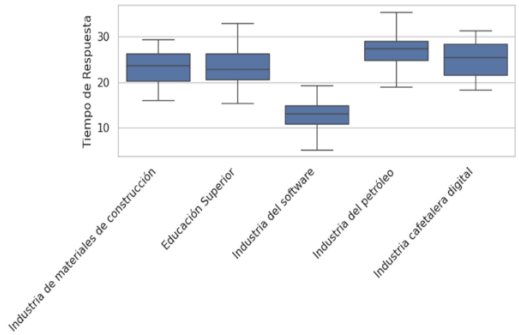


Figura 5:
Gráfico de caja del tiempo de respuesta ante incidentes de violación de la seguridad informática (2025).



Análisis cualitativo

La investigación recoge los desafíos, las estrategias y la cultura organizacional, refiere Miller (2017), de las 5 industrias estudiadas de manera cualitativa. Para lograrlo, el análisis contempla entrevistas y exploración documental de políticas, artículos y marcos legales.

Industria de Materiales de Construcción

Los desafíos encontrados en esta importante industria, son:

1. Necesidad de personal especializado en ciberseguridad.
2. Pobre inversión en las tecnologías de punta para la ciber defensa.
3. No hay una conciencia clara de los riesgos en las redes.

Estrategias Adoptadas para mitigar los riesgos son:

4. Ejecución de firewalls.
5. Capacitación al personal.
6. Adopción de un esquema estandarizado para la seguridad informática.

En cuanto a cultura en la organización, la industria de materiales de la construcción usa un tipo de cultura reactiva concentrada en la operatividad y no en la estrategia.

Educación Superior

Los desafíos de esta denominada industria en el sector de la educación, son:

1) La enorme demanda de redes facilita los ataques cibernéticos.
2) No existen políticas uniformes entre facultades, tanto de pre como de posgrados, mientras sí hay diversidad de estudiantes, docentes y administrativos.

Se han implementado grupos de seguridad, autenticación multi fator y estrategias de generación de conciencia sobre las vulnerabilidades de las redes en el sector.

Con respecto a la cultura organizacional, no existe un consenso que permita agrupar los diferentes criterios sobre la seguridad informática en una sola visión, aunque sí es cierto que el espíritu colaborador es palpable.

Industria del Software

Esta acelerada manufactura, en su prisa por el constante lanzamiento de nuevos productos y servicios, presenta una alta vulnerabilidad de sus códigos fuentes. Para mitigar las amenazas, se ha tomado como patrón el enfoque DevSecOps, integrando la seguridad, redacta Microsoft. (s.f.), en todas las fases del ciclo de vida del desarrollo de los productos y servicios de software y compartiendo la responsabilidad entre el equipo de desarrollo, los de operaciones y los encargados de la ciber seguridad.

Los del software, a diferencia de otras manufacturas, posee una alta gnosis sobre la seguridad de la información. Son proactivos y concentrados en la mejora de la calidad de sus productos y servicios.

Industria del Petróleo

El tamaño de la industria, su relevancia a nivel internacional y su importancia económica y energética global la hacen especialmente vulnerable a amenazas locales, regionales y geopolíticas (Energy Outlook, 2024).
Las estrategias adoptadas por el petróleo son:

1. Segmentación de las redes OT/IT.
2. Ejercicios de simulacros de ataques cibernéticos.
3. Cumplimiento de las normativas internacionales [NIST / ISO 27001].

La industria del petróleo, al ser de alto riesgo, ha creado con el paso de los años una cultura empresarial lista a cumplir las normas vigentes y la gestión de riesgos.

Industria Cafetalera

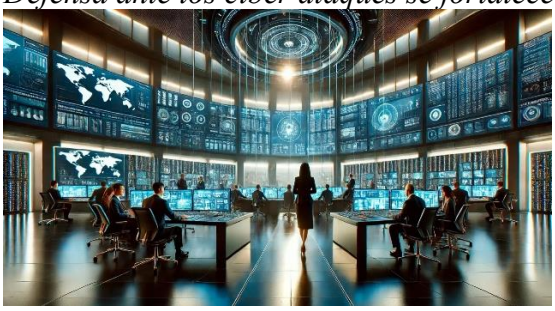
Los cafeteros presentan múltiples desafíos específicos, al tener una digitalización nueva. Eso conlleva falta de políticas concretas y una dependencia de servicios en la red negociado con proveedores externos, asumiendo riesgos de independencia operativa, seguridad de la información y sostenibilidad (Organización Internacional del Café, 2023).
Estrategias Adoptadas
Adopción de plataformas seguras, capacitación básica y externalización de servicios de ciberseguridad.
Cultura Organizacional
Cultura emergente en ciberseguridad, con interés creciente pero aún limitada institucionalización.

Línea de tiempo de los principales ciberataques a nivel mundial 2010-2025.

Aunque se escogió una población de 5 industrias diferentes entre sí, el mundo ha sido testigo de años de ataques cibernéticos a grandes empresas, emprendimientos de todo tipo, marcas de tecnología, plataformas financieras, gobiernos y demás. Los clientes, por millones, se han visto afectados en sus datos personales y financieros.
Tratando de definir las principales afectaciones a lo largo del tiempo, tenemos una muy resumida línea de tiempo.
2010 – La plataforma informática social WikiLeaks, publicó lo que se conoce como la mayor exposición de documentación secreta de la historia. Se expusieron más de 250,000 notas del Departamento de Estado de los Estados Unidos (WikiLeaks, 2010).
2011 – Sony PlayStation Network sufrió el hackeo de más de 77 millones de cuentas de usuario, sacando de servicio a la plataforma por más de 20 días (García, 2021).
2012 – Un poderoso Malware echó abajo los datos en 30,000 estaciones de trabajo de Shamoon en Arabia Saudí.
2013 – Target. En diciembre, no tan solo fue expuesta la información de aproximadamente 70 millones de clientes, sino que unos 40 millones de tarjetas de crédito y débito, resultaron envueltas en el ciberataque (Weiss & Miller, 2015).
2014 – eBay. Ciberataque que comprometió información de 145 millones de usuarios (CNBC, 2014).

2015 – Interferencia en Elecciones de EE.UU. Hackeo de correos electrónicos del Comité Nacional Demócrata, afirma (BBC Mundo, 2016), atribuido a actores rusos como APT28 y APT29.
2016 – La plataforma de citas adultas Friend Finder Networks, soportó que más de 400 millones de usuarios fueran expuestos y que se considerara como una de las mayores violaciones en la historia de la seguridad informática. Las plataformas objetos del ataque, cita (Infobae, 2016), incluyeron AdultFriendFinder.com, Cams.com, Penthouse.com y otras muchas, sacando a la luz correos electrónicos, contraseñas y datos de cuentas que habían sido eliminadas, pero se mantenían en la base de datos.
2017 – Uber. Robo de datos de 57 millones de usuarios y conductores, ocultado durante más de un año.
2018 – Cambridge Analytica. Uso indebido de datos de 87 millones de usuarios de Facebook para influir en elecciones.
2019 – Facebook. Exposición de más de 540 millones de registros de usuarios en servidores públicos.
2021 – Colonial Pipeline (EE.UU.). Ransomware provocó el cierre del mayor oleoducto de productos refinados en EE.UU.
2024–2025 Se ha comprobado un incremento inusual en los ciberataques, que no solo incluye industrias, sino que se contienen infraestructuras, sistema de salud y gobiernos mundiales. Se cifra en más de un 34% el incremento de los mismos (Redacción, 2025).

Figura 3:
Defensa ante los ciber ataques se fortalece a nivel mundial.



Estadísticas globales. Respuesta a las agresiones.

Las industrias en el mundo han comenzado a implementar acciones efectivas para fortalecer la seguridad informática. Concretamente en Latinoamérica, en 2025 alrededor del 78% de las empresas han aumentado los gastos aplicados a modernizar la ciberseguridad.
Uno de los ejemplos más importantes a nivel global son los centros de Operaciones de Seguridad (SOC). Estas unidades dentro de las industrias, se encargan de monitorear, detectar, analizar y eliminar amenazas de a la seguridad informática en tiempo real (Scapicchio et al., 2024).

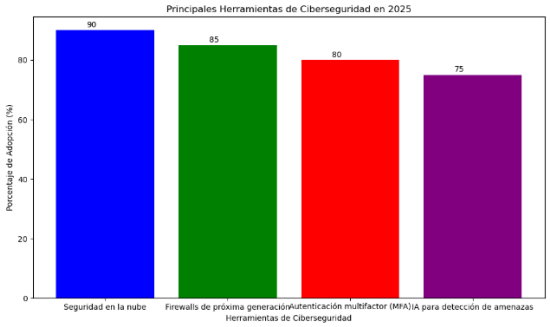
REVISTA FORMACIÓN ESTRATÉGICAISSN 2805-9832
Vol. 10 Núm. 2 (2024)
Recibido agosto 2024 –Aceptado enero 2025

La IA protagoniza la primera línea de defensa en aproximadamente el 62% de las industrias. Detectar peligros en tiempo real, acorta la respuesta en un 40%. IA generativa como barrera y respuesta contra los ciber delincuentes, está ganando terreno (Romero, 2024).
Los dispositivos **IO**T suman el 35% de las fallas de seguridad en la manufactura. Muchas conexiones a los sensores, cámaras y terminales, se encuentran sin autenticación robusta ni seguridad informática.

Figura 4:
Checklist de las principales herramientas de ciberseguridad empresariales.

El sector de la investigación médica tiene serios problemas de hackeo, sobre todo los laboratorios. La respuesta ha sido el incremento de la autenticación biométrica en un 45%. El uso de escáneres de retina, desestimula la intrusión (Manaure, 2025).
Las auditorias para revisar el cumplimiento de los estándares de la protección de datos han alcanzado la cifra del 64% en el entorno empresarial latino. Este tema, aparejado a la cultura en la seguridad, concientizan a las empresas y su responsabilidad al frente de los clientes. Por demás, disminuyen enormemente las posibilidades de los ciberataques camuflados.

Figura 4:
Principales herramientas de ciberseguridad 2025.



REVISTA FORMACIÓN ESTRATÉGICAISSN 2805-9832
Vol. 10 Núm. 2 (2024)
Recibido agosto 2024 –Aceptado enero 2025

Seguridad en la nube: 90%
Firewalls: 85%
Autenticación multifactorial: 80%
IA para amenazas:75%

1. CONCLUSIÓN

La protección frente a los ataques cibernéticos es una prioridad universal. Para ellos, la industria tiene que implementar estrategias integrales de ciberseguridad, donde se compongan etiquetas de seguridad, se encripten los datos y se proteja la investigación.
Paralelamente, resulta prioritario la ejecución permanente de las auditorías de seguridad, con el fin de evaluar fragilidades en el software y hardware que se usan comúnmente en los procesos productivos.
Las nuevas graduaciones profesionales deben formarse en el conocimiento de los principios sobre ciberseguridad. Solución Tecnológica Propósito
Personal docente, estudiantes de pregrado y posgrado y personal administrativo, deben ser partícipes de los programas instructivos sobre seguridad informática. Debe ser la regla, establecer normativas sobre el uso y la protección de datos. Igualmente es debe colaborar con expertos para proteger las innovaciones.
La sostenibilidad va de la mano con la ciberseguridad. El desarrollo empresarial debe ser sostenible, pero seguro frente al chantaje digital.
Para ejercer el control sobre los riesgos de ciberseguridad, el empresariado debe implementar soluciones tecnológicas eficientes.

Figura 5:
Principales soluciones tecnológicas y sus ventajas.

TECNOLOGÍA	DESCRIPCIÓN	VENTAJAS	APLICACIÓN
BIOMETRÍA	Verificación por huella, retina o rostro.	Alta seguridad, difícil de falsificar.	Laboratorios, bancos.
CIFRADO DE DATOS	Codifica datos para acceso solo autorizado.	Protege en tránsito y reposo.	Nube, comunicaciones.
ZERO TRUST	No se confía en ningún usuario por defecto.	Control estricto, segmentación.	Redes corporativas.
EDR/XDR	Detecta y responde a amenazas en tiempo real.	Respuesta rápida, visibilidad total.	Infraestructura crítica.
BLOCKCHAIN	Registro distribuido e inmutable.	Trazabilidad, integridad de datos.	Logística, salud, contratos.

Es importante, además, establecer lazos de colaboración con la IA, para evaluar predictivamente las vulnerabilidades y, con ello, establecer estrategias de respuestas certeras. En el caso concreto de la educación y otros, se deben establecer centinelas de IA para la protección de la información personal y académica del estudiante y de los servicios académicos.

Muchos países están adoptando marcos similares para garantizar que la IA sea ética, segura y no discriminatoria.

Resumiendo; la seguridad informática en la industria actual, demanda una combinación entre tecnología, políticas, conciencia y colaboración. Las empresas deben crear estrategias basadas en las amenazas presentes y futuras, considerando el fortalecimiento y capacidad humana y la internacionalización de los esfuerzos para afrontar los retos presentes y futuros.

Referencias bibliográficas

Álvarez, A. D., & Ospino, J. O. (2020). Evaluación de propiedades físico-químicas y mecánicas del adobe elaborado con cal para su uso en la construcción sostenible. REVISTA COLOMBIANA DE TECNOLOGIAS DE AVANZADA (RCTA), 1(35), Article 35. https://doi.org/10.24054/rcta.v1i35.47

Atlantic International University. (2024, mayo 23). La importancia de la seguridad en la era digital. https://www.aiu.edu/es/blog/la-importancia-de-la-seguridad-en-la-era-digital/
BBC Mundo. (2016, diciembre 17). Cómo fue el «hackeo» de piratas informáticos de Rusia durante las elecciones de Estados Unidos. BBC News Mundo. https://www.bbc.com/mundo/noticias-internacional-38350244

Energy Outlook, 2024 Edition. (2024). BP Energy Outlook 2024. 2024 Edition, 55.
Cafetero. (2025, mayo 21). >> Mercado del Café 2025: Análisis Completo con las Tendencias y Precios. Cortado con Hielo. https://cortadoconhielo.com/curiosidades/cafe-mercado-2025-datos-informe/

Carrero, N. S. S., Quintana, N. M. A., & Jaimes, L. M. S. (2022). Lineamientos desde la industria 4.0 a la educación 4.0: Caso tecnología IoT. REVISTA COLOMBIANA DE TECNOLOGIAS DE AVANZADA (RCTA), 1(39), Article 39. https://doi.org/10.24054/rcta.v1i39.1379

CNBC. (2014, mayo 22). Hackers raid eBay in historic breach, access 145M records. CNBC. https://www.cnbc.com/2014/05/22/hackers-raid-ebay-in-historic-breach-access-145-mln-records.html

Del Canto, E., & Silva Silva, A. (2013). Metodología cuantitativa: abordaje desde la complementariedad en ciencias sociales. Revista de Ciencias Sociales (Cr), (141), 25–34. Universidad de Costa Rica. https://www.redalyc.org/pdf/153/15329875002.pdf[1](https://www.redalyc.org/pdf/153/15329875002.pdf)

Drmunozcl. (2025, abril 7). Ley de privacidad del consumidor de California (CCPA). InfoProtección. https://www.infoproteccion.com/leyes-ciberseguridad/leyes-ciberseguridad-usa/ley-privacidad-consumidor-california-ccpa/

Estadística, P. y. (2021, diciembre 5). Diagrama de caja y bigotes (boxplot). Probabilidad y Estadística. https://www.probabilidadyestadistica.net/diagrama-de-caja-y-bigotes-boxplot/
EUR-LEX. (2022, enero 7). Reglamento general de protección de datos (RGPD). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:310401_2

Fernández, M. Á., & Pajares, R. (2017). La digitalización del mundo industrial. Economía Industrial, (405), 41–45. https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/FERNANDEZ%20Y%20PAJARES.pdf

Flórez, J. E. M., & Salazar, D. P. M. (2020). Arquitectura hardware/software para un prototipo de pozo inteligente en un campo petrolero maduro. REVISTA COLOMBIANA DE TECNOLOGIAS DE AVANZADA (RCTA), 2(36), Article 36. https://doi.org/10.24054/rcta.v2i36.27

Flores, R. (2025). Estudio de métodos mixtos en formato APA (Profesional). APA.org.es. https://apa.org.es/apa-pautas-de-estilo-y-gramatica/investigacion-y-publicacion/estudio-metodos-mixtos-formato-apa-profesional/

Forbes, R. (2019, noviembre 18). Las consecuencias de un ciberataque: Caso Pemex • Red Forbes • Forbes México. https://forbes.com.mx/las-consecuencias-de-un-ciberataque-caso-pemex/

Forbes, S. (2021, diciembre 15). Seis casos de ciberataque que marcaron el 2021. https://forbescentroamerica.com/2021/12/15/seis-ciberataques-que-marcaron-el-2021

García, D. M. (director). (2021, octubre). The 2011 PlayStation Network Hack – What Actually Happened? [Video recording]. https://wsswired.com/4837/entertainment-3/the-2011-playstation-network-hack-what-actually-happened/

Infobae. (2016, noviembre 14). Hackearon los datos de 400 millones de usuarios de «la comunidad más grande del mundo de sexo y libertinaje». https://www.infobae.com/america/tecno/2016/11/14/adult-friend-finder-network-hackearon-los-datos-de-400-millones-de-usuarios-en-un-ataque-a-una-web-de-citas-para-sexo-casual/

Landauer, M., Skopik, F., Stojanović, B., Flatscher, A., & Ullrich, T. (2024). A review of time-series analysis for cyber security analytics: From intrusion detection to attack prediction. International Journal of Information Security, 24(1), 3. https://doi.org/10.1007/s10207-024-00921-0

Manaure, A. (2025, enero 24). Autenticación biométrica: El escudo ante las ciberamenazas. CIOAL The Standard IT. https://thestandardcio.com/2025/01/24/autenticacion-biometrica-el-escudo-ante-las-ciberamenazas/

Malatji, M., & Tolah, A. (2025). Artificial intelligence (AI) cybersecurity dimensions: A comprehensive framework for understanding adversarial and offensive AI. AI and Ethics, 5(2), 883-910. https://doi.org/10.1007/s43681-024-00427-4

Márquez Díaz, J., Moreno, A. P., Rodríguez, L. C., & Ramírez, L. B. (2024). Industria 4.0. Internet de las Cosas: Ciberseguridad y aplicaciones. UCundinamarca. https://repositorioctei.ucundinamarca.edu.co/ingenieria/3

Microsoft. (s.f.). ¿Qué es DevSecOps? Definición y procedimientos recomendados. Microsoft. Recuperado el 11 de junio de 2025, de https://www.microsoft.com/es-mx/security/business/security-101/what-is-devsecops

Miller, J. (2017). Qualitative research methods: Interviews and document analysis in organizational studies. Journal of Organizational Inquiry, 26(3), 45–59

Muñoz, A. B. (2024). Educar y proteger: Análisis de la educación en ciberseguridad para combatir la ciberdelincuencia. Revista de Educación y Derecho, 30, Article 30. https://doi.org/10.1344/REYD2024.30.44082

Nordström, F., Gawad, P., & Nowarski, A. (2006). La ciencia de la fabricación. ABB, 11.
Organización Internacional del Café. (2023). Coffee Development Report 2022–23: The Future of Coffee in a Digital World. International Coffee Organization. Recuperado de https://www.ico.org

Perlroth, N. (2012, octubre 24). In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. The New York Times. https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

Puentes, M. D. P. R., Parada, C. J., & Pabón, J. L. L. (2022). Estructuras desglosadas de trabajo (EDT) en la gestión de alcance de proyectos de desarrollo de software. REVISTA COLOMBIANA DE TECNOLOGIAS DE AVANZADA (RCTA), 1(39), Article 39. https://doi.org/10.24054/rcta.v1i39.1375

Redacción, T. (2025, marzo 17). Sectores críticos en riesgo por aumento de ciberataques. https://t21.pe/sectores-criticos-riesgo-aumento-ciberataques

Rodrigo, R. (2020, septiembre 30). Derrame de petróleo de Deepwater Horizon: Causas, efectos y hechos. Estudyando. https://estudyando.com/derrame-de-petroleo-de-deepwater-horizon-causas-efectos-y-hechos/

Romero, J. (2024). El uso de IA generativa para ciberdefensa toma cuerpo. PwC. https://www.pwc.es/es/publicaciones/transformacion-digital/global-digital-trust-insights-2024.html

Royakkers, L., Timmer, J., Kool, L., & van Est, R. (2018). Societal and ethical issues of digitization. Ethics and Information Technology, 20(2), 127-142. https://doi.org/10.1007/s10676-018-9452-x

Rueda, K. S. C. (2022). Aplicación de redes neuronales artificiales para el pronóstico de precios de café. REVISTA COLOMBIANA DE TECNOLOGIAS DE AVANZADA (RCTA), 1(39), Article 39. https://doi.org/10.24054/rcta.v1i39.1403

Scapicchio, M., Downie, A., & Finio, M. (2024, marzo 15). ¿Qué es un centro de operaciones de seguridad (SOC)? | IBM. https://www.ibm.com/es-es/topics/security-operations-center
Westerman, G., Kane, G. C., Woerner, S., & Ross, J. W. (2025). The path to digital transformation. MIT Sloan Management Review. https://sloanreview.mit.edu/the-path-to-digital-transformation/

Weiss, N. E., & Miller, R. S. (2015). The Target and Other Financial Data Breaches: Frequently Asked Questions.

WikiLeaks. (2010). WikiLeaks—Cablegate: 250,000 US Embassy diplomatic Cables. https://wikileaks.org/Cablegate-250-000-US-Embassy.html