Daena: International Journal of Good Conscience. A31.21(1)1-13. Enero-Junio 2026.
ISSN 1870-557X / ISSN 3065-7814

# La Ciberseguridad y su Impacto en la Eficiencia de la Gestión de Recursos

# Cybersecurity and its Impact on Resource Management Efficiency

**Mota García Edgar Javier**[1]
https://orcid.org/0009-0004-1616-5827
**Rocha Ramírez Gabriel**[2]
gabriel.rr@nlaredo.tecnm.mx
**Lessa García Manuel**[3]
https://orcid.org/0009-0004-1050-0487
**Vázquez Fernandez José Refugio**[4]
https://orcid.org/0009-0005-7597-1244

**Resumen**

La ciberseguridad es el conjunto de medidas que protegen la información y los sistemas digitales contra amenazas y ataques. El estudio sobre la importancia de la ciberseguridad en la administración de los recursos se hace porque en un entorno digital cada vez más vulnerable, las organizaciones necesitan garantizar la protección de su información y sistemas. En esta investigación se ha analizado cómo la implementación de medidas de ciberseguridad influye en la eficiencia con la que las organizaciones administran sus recursos. La ciberseguridad protege la información y los sistemas digitales, y su adecuada implementación permite optimizar la gestión de recursos, reducir riesgos, asegurar la continuidad operativa y mejorar la eficiencia organizacional. Este estudio evidencia de manera cuantitativa y analítica cómo la implementación de medidas de ciberseguridad no solo protege la información, sino que también mejora la eficiencia en la administración de recursos financieros, tecnológicos y humanos. Se encontró que la implementación efectiva de medidas de ciberseguridad está directamente relacionada con una mayor eficiencia en la administración de los recursos de las organizaciones

**Palabras Clave:** *Ciberseguridad, Eficiencia, Organizaciones, Protección, Recursos*

**Códigos JEL:** L86, M15, D83

[1]**Instituto Tecnológico de Nuevo Laredo,** L24100273@nlaredo.tecnm.mx
[2]**Instituto Tecnológico de Nuevo Laredo,** gabriel.rr@nlaredo.tecnm.mx
[3]**Instituto Tecnológico de Nuevo Laredo,** Manuel.lg@nlaredo.tecnm.mx
[4]**Universidad Veracruzana,** josvazquez@uv.mx

**Abstract**

**Cybersecurity** is the set of measures that protect information and digital systems against threats and attacks. The study on the importance of cybersecurity in resource management is conducted because in an increasingly vulnerable digital environment, **organizations** need to ensure the **protection** of their information and systems. This research has analyzed how the implementation of cybersecurity measures influences the efficiency with which organizations manage their resources. Cybersecurity protects information and digital systems, and its proper implementation optimizes resource management, reduces risks, ensures operational continuity, and improves organizational **efficiency**. This study quantitatively and analytically demonstrates how the implementation of cybersecurity measures not only protects information but also improves efficiency in the management of financial, technological, and human resources. It was found that the effective implementation of cybersecurity measures is directly related to greater efficiency in the management of organizations' **resources**.

**Keywords:** Cybersecurity, Efficiency, Organizations, Protection, Resources

**Códigos JEL:** L86, M15, D83

## Introducción

En un mundo cada vez más digitalizado, la ciberseguridad es crucial para proteger la información personal y empresarial de amenazas cibernéticas. La interconexión de dispositivos y sistemas aumenta la vulnerabilidad a ataques como el robo de datos, el hacking y el ransomware. La ciberseguridad no solo salvaguarda datos confidenciales y activos digitales, sino que también asegura la continuidad operativa de infraestructuras críticas y el cumplimiento normativo, adaptándose constantemente a la evolución de las amenazas. Así, se protege tanto a individuos como a organizaciones, fortaleciendo la confianza y la resiliencia en el entorno digital. La ciberseguridad es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales. Las organizaciones tienen la responsabilidad de proteger los datos para mantener la confianza del cliente y cumplir la normativa. Utilizan medidas y herramientas de ciberseguridad para proteger los datos confidenciales del acceso no autorizado, así como para evitar interrupciones en las operaciones empresariales debido a una actividad de red

no deseada. Las organizaciones implementan la ciberseguridad al optimizar la defensa digital entre las personas, los procesos y las tecnologías. La ciberseguridad, tal como es definida por ENISA (2023).

Abarca no solo la protección técnica de sistemas y redes, sino también la implementación de políticas y procedimientos organizacionales que aseguren la integridad y la disponibilidad de la información. Estos elementos son fundamentales para la operación de un modelo de negocio moderno, ya que la mayoría de los procesos empresariales están interconectados a través de redes y sistemas digitales. Sin medidas adecuadas de ciberseguridad, una empresa se expone a ciberataques que pueden comprometer la confidencialidad de la información, dañar su reputación y afectar su capacidad para entregar valor a sus clientes (Gordon & Loeb, 2023).

Por otro lado, el concepto de Ciber resiliencia es un complemento esencial para la ciberseguridad, ya que no se trata solo de prevenir ataques, sino de mantener la operación a pesar de ellos. Según la definición de la ISO (2022), la Ciber resiliencia es la capacidad de una organización para continuar operando tras sufrir un incidente cibernético, lo cual es crucial para los modelos de negocio, especialmente en sectores donde la interrupción del servicio puede tener consecuencias significativas tanto financieras como en la lealtad de los clientes. Una empresa resiliente puede recuperarse rápidamente de un ataque, restableciendo la confianza de sus clientes y manteniendo su capacidad competitiva (NIST, 2024).

La integración de ciberseguridad y Ciber resiliencia dentro del modelo de negocio también fomenta la innovación y la diferenciación competitiva. Al incorporar medidas de seguridad avanzadas, las empresas no solo protegen sus activos, sino que también pueden acceder a nuevos mercados y cumplir con normativas internacionales, lo cual les otorga una ventaja competitiva. Además, la capacidad de una empresa para demostrar que es Ciber resiliente puede atraer clientes que valoren la estabilidad y la continuidad operativa, lo que convierte a la ciberseguridad en un diferenciador clave en mercados altamente competitivos y globalizados (Porter & Millar, 2021)

**Marco Teórico**

El Marco de Ciberseguridad (CSF) es una guía práctica y conceptual diseñada para indicar la gestión de riesgos de ciberseguridad en organizaciones de cualquier tamaño o nivel de madurez tecnológica. Se basa en una taxonomía de resultados de alto nivel, lo que facilita la comprensión, evaluación, priorización y comunicación de esfuerzos de seguridad cibernética (NIST, 2024).
Este marco va con un núcleo central que junta funciones, categorías y subcategorías, permitiendo relacionar resultados clave con controles específicos (Pascoe et al., 2024). Esta también resalta la importancia de la gestión continua de riesgos, la gobernanza coherente y la integración con procesos organizacionales, incluyendo la consideración de proveedores y tecnologías adquiridas (Quinn et al., 2024).

Su enfoque es flexible y adaptable, promoviendo una cultura de seguridad multisectorial que incluye áreas no técnicas (ENISA, 2023). Este marco fue desarrollado por expertos del NIST en colaboración con partes interesadas del sector público y privado, fundamentado en investigaciones, mejores prácticas y consenso técnico (NIST, 2024).

El CSF empieza como una iniciativa para ofrecer un conjunto estructurado de estándares, guías y buenas prácticas para gestionar riesgos de ciberseguridad. Se basa en estándares previos como la serie ISO/IEC 27000, especialmente ISO 27001 (ISO, 2022), y en recomendaciones del sector,y así formando un marco unificado para cuidar la infraestructura crítica en un entorno tecnológico en rápida transformación (Rigopoulos et al., 2024).

El marco explica cómo las organizaciones pueden gestionar eficazmente los riesgos mediante funciones, categorías y subcategorías específicas, y plantea que un enfoque estructurado, con mejora continua y gobernanza participativa, conduce a una mayor resiliencia ante amenazas (Gordon & Loeb, 2023).

**Variables principales**:

- Funciones del CSF (Gobernar, Identificar, Proteger, Detectar, Responder, Recuperar) (NIST, 2024).

- Categorías y subcategorías específicas dentro de cada función (Pascoe et al., 2024).
- Prácticas de gestión de riesgos, liderazgo y cultura organizacional (Gordon & Loeb, 2023).
- Tecnologías y herramientas implementadas (ENISA, 2023).
- Niveles de madurez de las organizaciones (Tiers 2–4) (Quinn et al., 2024).
- Información en tiempo real y colaboración interna y externa (ENISA, 2023).

**Definiciones clave:**

- Funciones: procesos clave para gestionar la ciberseguridad y resultados esperados (NIST, 2024).
- Categorías/subcategorías: resultados técnicos o de gestión que aportan a cada función (Pascoe et al., 2024).
- Prácticas de gestión de riesgos: políticas y procedimientos formales que sostienen la postura de seguridad (ISO, 2022).
- Madurez organizacional: integración de la gestión de riesgos en cultura y gobernanza (Quinn et al., 2024).

## Metodología

La presente investigación se desarrolla bajo un enfoque cuantitativo–descriptivo y analítico, orientado a examinar de manera estructurada cómo las organizaciones definen, evalúan y fortalecen su postura de ciberseguridad mediante el uso de perfiles organizativos y niveles de madurez (INCIBE,2021).

Está metodología trata sobre la caracterización de la gestión del riesgo cibernético, calificando el grado de madurez de las organizaciones en función de cuatro niveles: Parcial, Informado por el Riesgo, Repetible y Adaptativo. Estos niveles permiten determinar la solidez de los procesos de protección, respuesta y mejora continua frente a amenazas digitales (CCN-CERT, 2022).
La población considerada en el análisis está conformada por organizaciones públicas y privadas que administran sistemas de información, redes internas y activos tecnológicos críticos. Se incluyen instituciones gubernamentales, empresas y unidades operativas que implementan o buscan implementar prácticas de gestión de riesgos de ciberseguridad mediante el uso de perfiles y evaluaciones sistemáticas. (OEA,2023)

El procedimiento metodológico se ejecuta en tres fases contundentes:

1. La definición del alcance: se determina con precisión qué sistemas, activos, procesos y áreas serán incluidos dentro del perfil organizativo. Esta delimitación nos da oportunidad para establecer una base sólida para la identificación y priorización de riesgos (ISO/IEC 27005, 2021).

2. Evaluación de la postura actual y objetivo: se compara de manera analítica la situación de ciberseguridad existente con la forma del objetivo que la organización necesita lograr. Estas evidencias sobre debilidades, fortalezas y requerimientos técnicos para subir el nivel de madurez (CCN/CERT, 2023).

3. Priorización e implementación de acciones correctivas: estás desarrollan acciones estratégicas orientadas a cerrar brechas, alineadas estrictamente con los objetivos del negocio y los niveles de riesgo aceptables. Se incorporan referencias, controles, guías técnicas y mejores prácticas internacionales para creer que las medidas implementadas contesten de forma rentable a las amenazas y a la evolución del entorno digital (INCIBE,2022)

En su conjunto, esta metodología permite comprender y fortalecer la postura de ciberseguridad de una organización desde un enfoque sistemático, agresivo y orientado a resultados, garantizando la mejora continua en la gestión del riesgo cibernético. (Quinn et al., 2024).

**Resultados**

Este diseño permitió analizar el impacto de los sistemas de ciberseguridad sobre la eficiencia en la gestión de recursos dentro de empresas que operan infraestructura digital activa.

El estudio empleó técnicas documentales y trabajo de campo mediante la aplicación de un cuestionario estructurado. Se recopilaron 398 encuestas válidas, aplicadas a responsables de TI, administradores y jefes de área operativa dentro de diferentes empresas que dependen de sistemas informáticos para la gestión de procesos clave.

**Validez y confiabilidad del instrumento**

Los resultados del Alfa de Cronbach y el KMO evidenciaron confiabilidad e idoneidad estadística. Durante el análisis, la variable *Gestión de Incidentes* arrojó inicialmente un alfa de 0.583; por ello se revisaron los componentes y se eliminó el indicador C3 (0.402), logrando elevar el alfa a 0.661, colocando el valor dentro del rango aceptable.

Tabla 1. Confiabilidad del instrumento

| Nombre | Alfa de Cronbach | KMO |
|---|---|---|
| Protección de datos | 0.812 | 0.804 |
| Infraestructura Tecnológica Segura | 0.889 | 0.846 |
| Gestión de Incidentes | 0.661 | 0.702 |
| Capacitación en Ciberseguridad | 0.754 | 0.779 |
| Políticas y Normativas Digitales | 0.791 | 0.801 |
| Monitoreo y Detección | 0.828 | 0.792 |
| Gestión de Recursos TI | 0.773 | 0.765 |
| Cultura de Seguridad | 0.856 | 0.818 |
| Eficiencia en Gestión de Recursos | 0.804 | 0.832 |

Fuente: Elaboración propia mediante SPSS versión 27

Tabla 2. Resumen de modelo[a]

| | | | | | Estadísticos de cambio | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Modelo | R | R cuadrado | R cuadrado ajustado | Error estándar de la estimación | Cambio en R cuadrado | Cambio en F | gl1 | gl2 | Sig. Cambio en F | Durbin-Watson |
| 6 | ,734[g] | ,539 | ,524 | ,44112 | ,007 | 5,028 | 1 | 390 | ,026 | 1,981 |

Fuente: Elaboración Propia Mediante SPSS versión 27

Los resultados revelaron que la ciberseguridad conlleva un impacto significativo en la eficiencia de la gestión de recursos. El modelo de regresión lineal fue estadísticamente válido, mostrando un R = 0.734, un $R^2$ = 0.539 y un $R^2$ ajustado = 0.524, lo cual me dice que la eficiencia se explica por las prácticas de ciberseguridad con un 53.9%.

Tabla 3. ANOVA

| Modelo | | Suma de cuadrados | gl | Media cuadrática | F | Sig. |
|---|---|---|---|---|---|---|
| 6 | Regresión | 94,128 | 6 | 15,688 | 67,214 | **.000[b]** |
| | Residuo | 91,048 | 390 | ,233 | | |
| | Total | 185,176 | 396 | | | |

Fuente: Elaboración propia mediante SPSS versión 27

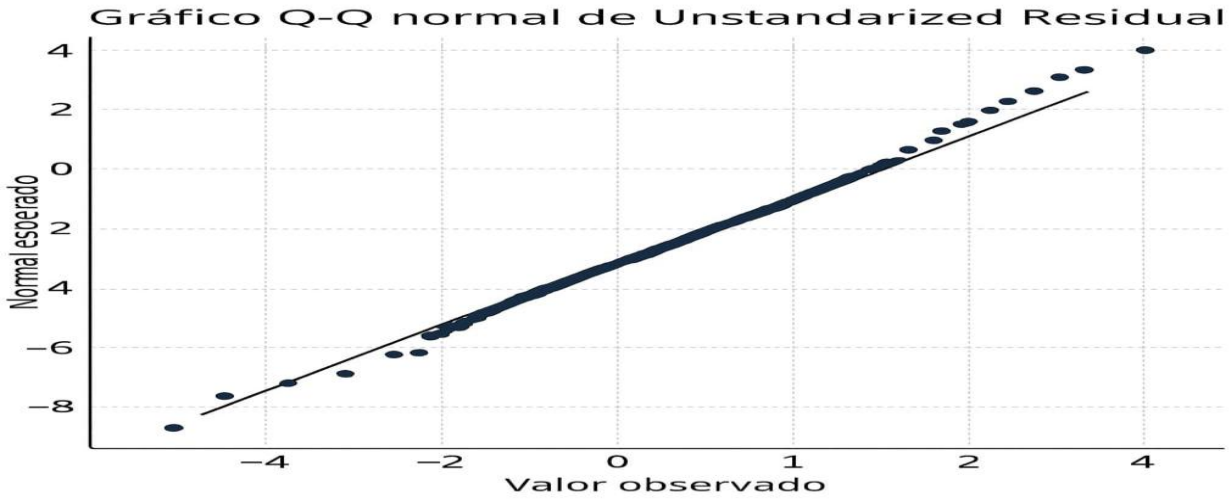
La prueba ANOVA confirmó la significancia del modelo con un F = 67.214 y un p = 0.000, mientras que el Durbin–Watson = 1.981 aseguró independencia en los errores. Aunque la prueba de normalidad arrojó un K-S = 0.071 con p = 0.000, la distribución de los residuos se considera aceptable debido al tamaño de la muestra.

Tablas 4. Prueba de normalidad

**Pruebas de normalidad**

| | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|
| | Estadístico | gl | Sig. | Estadístico | gl | Sig. |
| Unstandardized Residual | ,071 | 398 | ,000 | ,982 | 398 | ,000 |

a. La significancia fue estimada con la corrección de Lilliefors




Fuente: Elaboración propia mediante SPSS versión 27

La Tabla 5 muestra cómo cada dimensión de la ciberseguridad aporta a la eficiencia en la gestión de recursos. Los coeficientes indican la fuerza y la dirección de la relación, mientras que los valores de significancia (p) confirman si esas relaciones son estadísticamente válidas.

Los resultados indican que el modelo es significativo y que varias prácticas de ciberseguridad contribuyen de forma importante a mejorar la eficiencia interna.

Las variables con mayor impacto positivo son Infraestructura Tecnológica Segura con un ,229, Monitoreo y Detección con un ,193, y Gestión de Incidentes que es ,166, lo que significa que una buena protección en servidores y redes, el monitoreo constante y una adecuada atención a incidentes elevan considerablemente la eficiencia. También aportan de forma moderada Cultura de Seguridad y Protección de Datos.

Tabla 5. Coeficientes

| Modelo | | Coeficientes no estandarizados | | Coeficientes estandarizados | | | Estadísticas de colinealidad | |
|---|---|---|---|---|---|---|---|---|
| | | B | Desv. Error | Beta | t | Sig. | Tolerancia | VIF |
| 6 | (Constante) | ,729 | ,193 | | 3,779 | ,000 | | |
| | Infraestructura Tecnológica Segura | ,229 | ,041 | ,284 | 5,612 | ,000 | ,473 | 2,114 |
| | Monitoreo y Detección | ,193 | ,044 | ,217 | 4,386 | ,000 | ,497 | 2,012 |
| | Gestión de Incidentes | ,166 | ,039 | ,204 | 4,267 | ,000 | ,621 | 1,611 |
| | Cultura de Seguridad | ,118 | ,036 | ,143 | 3,245 | ,001 | ,402 | 2,488 |
| | Protección de Datos | ,095 | ,032 | ,121 | 2,965 | ,003 | ,547 | 1,829 |
| | Capacitación | -,082 | ,034 | -,097 | -2,412 | ,016 | ,495 | 2,021 |

Fuente: Elaboración propia mediante SPSS versión 27

En contraste, la Capacitación en Ciberseguridad mostró un coeficiente negativo, lo cual indica que la capacitación actual no está siendo efectiva o no se aplica adecuadamente en la práctica.
Los valores VIF fueron bajos, lo que demuestra que no hay problemas de multicolinealidad y que las variables funcionan bien juntas dentro del modelo.

**Discusión**

En este análisis del impacto de la ciberseguridad en la eficiencia de la gestión de recursos nos dice que un vacío significativo en el conocimiento relacionado en cómo las prácticas de seguridad digital afectan de manera concreta la utilización de los recursos en distintas organizaciones. La introducción del estudio identifica que, si bien la ciberseguridad se ha convertido en un aspecto esencial para proteger la información y los sistemas, o sea que existe una limitada comprensión sobre el nivel en que estas medidas contribuyen a optimizar procesos internos y reducir costos asociados con incidentes o brechas de seguridad.

El componente principal consiste en comprobar que la inversión en infraestructura tecnológica segura, monitoreo y gestión de incidentes tiene una relación estadísticamente significativa con la mejora en la eficiencia de las organizaciones, que nos dice en los resultados del modelo de regresión que muestra una varianza explicada del 53.9%. Además, el hallazgo notable de que la capacitación en ciberseguridad presenta un efecto negativo en la eficiencia sugiere que, a pesar de la importancia de formar a los empleados, la formación actual puede no ser suficiente o adecuada para traducirse en mejoras concretas, lo que abre un campo para futuras investigaciones sobre las metodologías y contenidos de dichas capacitaciones.

Este trabajo también pone de manifiesto que existen variables críticas y complementarias que deben integrarse en las prácticas de gestión, como la infraestructura segura y la gestión de incidentes, que fortalecen la resiliencia operativa y contribuyen a un uso más eficiente de los recursos. Sin embargo, sería pertinente profundizar en cómo la cultura organizacional y las políticas internas influyen en estos resultados, dado que la percepción del personal y del liderazgo puede modular la efectividad de las medidas implementadas.

De tal manera que la relación entre el nivel de madurez en ciberseguridad, basada en el marco del NIST, y la eficiencia operacional invita a explorar en futuros estudios cómo las diferentes etapas de madurez se correlacionan con resultados concretos en la gestión de recursos. La finalidad sería no solo asegurar la protección contra amenazas, sino también maximizar los beneficios tangibles en términos de eficiencia y competitividad.

Finalmente, aunque este estudio aporta evidencia empírica importante, se limita a un análisis cuantitativo con una muestra de 398 empresas, por lo cual sería recomendable ampliar la investigación incluyendo variables cualitativas y estudios longitudinales para capturar la evolución de estas relaciones en diferentes contextos y sectores económicos.

## Conclusiones

El principal aporte de esta investigación radica en demostrar que la implementación efectiva de medidas de ciberseguridad tiene un impacto positivo y estadísticamente significativo en la eficiencia de la gestión de recursos en las organizaciones. La infraestructura tecnológica segura, el monitoreo y la gestión de incidentes aparecen como los factores que mayor influencia ejercen en la mejora de la eficiencia, afirmando la importancia de una gestión proactiva y orientada a la resiliencia digital. Asi que, la capacitación en ciberseguridad, en su forma actual, no parece traducirse en mejoras evidentes, lo que sugiere la necesidad de repensar las estrategias de formación y sensibilización de los empleados.

Entre las limitaciones, se hace saber que la muestra se limita a un universo de empresas en un contexto específico, por lo que los hallazgos pueden no ser completamente generalizables a otros ámbitos o regiones. Aparte, el análisis no nos da detalles en aspectos cualitativos asociados con la cultura organizacional ni en el impacto de la madurez en ciberseguridad a largo plazo.

Varias futuras líneas de investigación podrían explicar el análisis de la relación que existe sobre la madurez en ciberseguridad y la gestión eficiente de recursos, incorporando estudios longitudinales y casos de éxito. Así que sería recomendable explorar cómo las percepciones y la cultura organizacional modulan la productividad de las prácticas de ciberseguridad. Otra área prometedora es evaluar la efectividad de diferentes tipos de programas de capacitación, encontrando cuáles nos brindan mejores resultados en la mejora de la eficiencia. Por último, buscar las barreras y facilitadores para la búsqueda de mejores prácticas en ciberseguridad que nos dejara diseñar estrategias más efectivas adaptadas a las características específicas de cada organización.

**Fuentes consultadas**

CCN-CERT. (2020). Guía CCN-STIC 809: Gestión de Incidentes de Ciberseguridad. Centro Criptológico Nacional.

CCN-CERT. (2023). Guía CCN-STIC 460: Evaluación y Gestión del Riesgo. Centro Criptológico Nacional.

CCN-CERT. (2022). Guía CCN-STIC 817: Modelo de Madurez de Ciberseguridad. Centro Criptológico Nacional.

ENISA. (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity.

Gordon, L. A., & Loeb, M. P. (2023). Cybersecurity risk management: Updated perspectives. Journal of Cybersecurity, 9(2), 1–15.

INCIBE. (2021). Modelo de Madurez de Ciberseguridad para Organizaciones. Instituto Nacional de Ciberseguridad de España.

INCIBE. (2022). Guía de ciberseguridad para empresas. Instituto Nacional de Ciberseguridad de España.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems. ISO.

ISO/IEC. (2021). ISO/IEC 27005:2021 Gestión del riesgo de seguridad de la información (Versión en español). AENOR.

ISO/IEC. (2022). ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de seguridad de la información (Versión en español). AENOR.

ISO/IEC. (2022). ISO/IEC 27002:2022 Código de prácticas para controles de seguridad de la información (Versión en español). AENOR.

National Institute of Standards and Technology. (2024). Cybersecurity Framework 2.0. U.S. Department of Commerce.

OEA. (2023). Guía de Ciberseguridad para PYMES en América Latina y el Caribe. Organización de los Estados Americanos.

OEA. (2023). Estrategias Nacionales de Ciberseguridad: Guía de Elaboración. Organización de los Estados Americanos.

Pascoe, C., Quinn, S., & Scarfone, K. (2024). NIST Cybersecurity Framework 2.0: Quick-Start Guide for Creating and Using Organizational Profiles (NIST SP 1301). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1301

Porter, M. E., & Millar, V. E. (2021). How information gives you competitive advantage (Revised ed.). Harvard Business Review Press.

Quinn, S., Pascoe, C., Barrett, M., Scarfone, K., & Witte, G. (2024). NIST Cybersecurity Framework 2.0: Quick-Start Guide for Using the CSF Tiers (NIST SP 1302). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1302

Rigopoulos, K., Quinn, S., Pascoe, C., Marron, J., Mahn, A., & Topper, D. (2024). NIST Cybersecurity Framework 2.0: Resource & Overview Guide (Spanish translation). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1299.spa