Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

VULNERABILIDAD E INFRAESTRUCTURA DE RED. UNA MIRADA DESDE LAS REPERCUSIONES EN LAS EMPRESAS

María Gil[4]

Resumen
Con el avance de la digitalización las organizaciones han experimentado una progresiva dependencia de los sistemas de gestión, así como de las tecnologías de la información y de la comunicación. Las herramientas que garantizan el funcionamiento de esa tecnología y de todos los sistemas de apoyo y control de gestión son las infraestructuras de red. Considerando la importancia del funcionamiento adecuado de la infraestructura de redes es importante no perder de vista las vulnerabilidades a las que se expone. Se ha hecho obligatorio la protección y vigilancia de toda la tecnología ante amenazas latentes. En el presente artículo se desarrolla una revisión sistemática y bibliográfica acerca del análisis de vulnerabilidades de infraestructura de red, empleado para ello las bases de datos IEEE, SCOPUS y Redalyc. Se determinó que el método más utilizado fue el análisis de tráfico, y la técnica más empleada el fuzzing de protocolos de red. Predominó el análisis de vulnerabilidades sobre protocolos de red y, por tanto, el análisis del componente de servicio. El análisis de vulnerabilidades en infraestructuras de red es un ámbito de investigación que tiene escasa documentación científica requiriendo especial atención el ámbito empresarial.

Palabras clave: análisis de redes, seguridad, vulnerabilidades de red, repercusiones en la empresa.

VULNERABILITY AND NETWORK INFRASTRUCTURE. A LOOK FROM THE REPERCUSSIONS ON COMPANIES

Abstract
With the advancement of digitalization, organizations have experienced a progressive dependence on management systems, as well as on information and communication technologies. The tools that guarantee the functioning of this technology and of all management support and control systems are network infrastructures. Considering the importance of the proper functioning of the network infrastructure, it is important not to lose sight of the vulnerabilities to which it is exposed. The protection and monitoring of all technology against latent threats has become mandatory. In this article, a systematic and bibliographic review of network infrastructure vulnerability analysis is developed, using the IEEE, SCOPUS, and Redalyc databases for this purpose. It was determined that the most used method was traffic analysis, and the most employed technique was network protocol fuzzing.

[4] Estudiante de Ingeniería en la Universidad Bicentenaria de Aragua (UBA), San Joaquín de Turmero, Aragua, Venezuela.

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

Vulnerability analysis of network protocols predominated and, therefore, the analysis of the service component. Vulnerability analysis in network infrastructures is a research field that has scarce scientific documentation, requiring special attention in the corporate sphere.

Keywords: Network Analysis, Security, Network Vulnerabilities, Repercussions on the Company.

Introducción

La vulnerabilidad en la infraestructura de red se ha consolidado como un tema crítico en el entorno actual de la ciberseguridad, principalmente debido a la creciente dependencia que las organizaciones han desarrollado hacia la tecnología para sostener sus operaciones diarias. Las infraestructuras de red, compuestas por una arquitectura compleja de dispositivos como routers, switches, firewalls y soluciones en la nube, representan los pilares fundamentales que garantizan el funcionamiento eficiente de los sistemas de gestión, la comunicación interna y el intercambio de datos corporativos.

Sin embargo, esta digitalización progresiva ha expuesto a las organizaciones a amenazas latentes, donde elementos esenciales para la operatividad se convierten en blancos primarios para ciberatacantes que explotan debilidades en el diseño, la configuración o el mantenimiento de los sistemas. La materialización de estas vulnerabilidades conlleva repercusiones significativas que trascienden el plano técnico, impactando directamente en la continuidad del negocio, la integridad de los activos, la reputación corporativa y, en última instancia, en la sostenibilidad financiera de la empresa.

A pesar de que el análisis de vulnerabilidades es una práctica fundamental para mitigar riesgos y proteger la operatividad, este ámbito de investigación presenta una escasez de documentación científica, lo que exige una atención especial desde el campo empresarial. Por lo tanto, el presente

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

artículo tiene como propósito desarrollar una revisión sistemática y bibliográfica acerca del análisis de vulnerabilidades de infraestructura de red, empleando como fuentes las bases de datos IEEE, SCOPUS y Redalyc.

A través de esta revisión, se exploran los métodos más empleados, tales como el análisis de tráfico y el fuzzing de protocolos, para finalmente establecer consideraciones estratégicas que permitan a las organizaciones fortalecer su postura de seguridad. La estructura del artículo se organiza abordando, en primer lugar, la conceptualización de la infraestructura y su evolución histórica, para posteriormente analizar los tipos de vulnerabilidades, sus repercusiones organizacionales y, finalmente, presentar las recomendaciones metodológicas para una gestión proactiva de riesgos.

Vulnerabilidad e infraestructura de red

La vulnerabilidad en redes se conceptualiza como cualquier debilidad técnica en el diseño, la implementación o el mantenimiento de los sistemas informáticos, que es susceptible de ser explotada por amenazas internas o externas. Según Schneier (2015), estas deficiencias ponen en riesgo directo la tríada de la seguridad de la información: integridad, confidencialidad y disponibilidad. Limones (2022) subraya que los fallos suelen originarse en errores humanos de configuración o fallos de programación en hardware y software, lo que convierte al análisis de vulnerabilidades en una práctica de gestión esencial para mantener la operatividad corporativa y proteger los sistemas ejecutados en dichas infraestructuras. Molina y Orozco (2020) refuerzan esta postura al señalar que, mediante técnicas especializadas, es posible identificar estas debilidades potenciales para diseñar estrategias preventivas que reduzcan el riesgo de ataques.

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

La infraestructura de red en una empresa

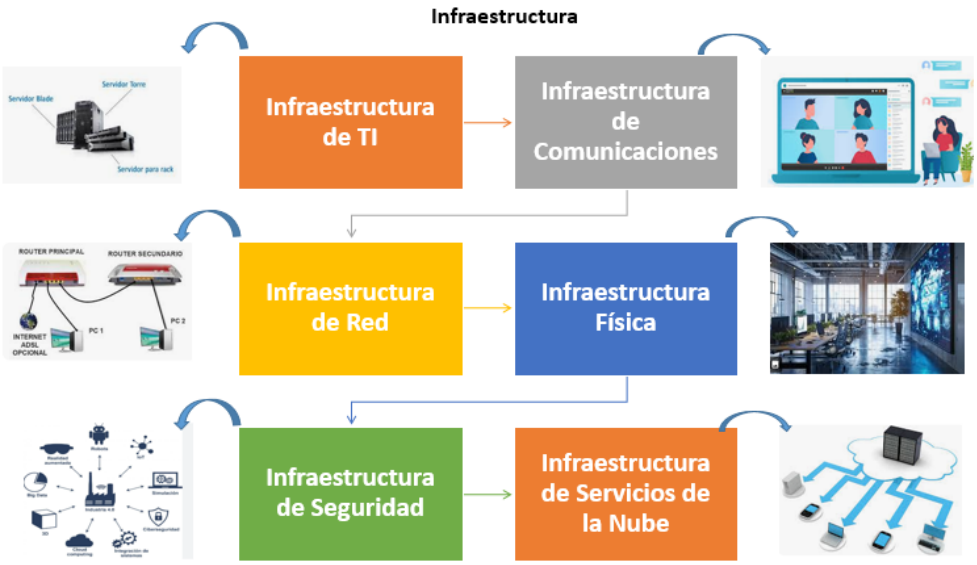
La infraestructura de red es el soporte sobre el cual se asienta el éxito competitivo de la empresa moderna. Siguiendo la clasificación de Melendez y Dávila (2018), esta se compone de una red interrelacionada de elementos:

- **Infraestructura de TI:** Integra los servidores, sistemas de almacenamiento y el *software* necesario para la gestión y manejo de datos.
- **Infraestructura de red:** Comprende los dispositivos activos (enrutadores, *switches*), así como el cableado y los protocolos que posibilitan la conectividad.
- **Infraestructura física:** Incluye las instalaciones, centros de datos y espacios físicos que soportan la operatividad.
- **Infraestructura de comunicaciones:** Abarca los sistemas de telefonía y videoconferencia, vitales para la colaboración interna.
- **Infraestructura de seguridad:** Integra sistemas de detección de intrusos (IDS), políticas de acceso y formación continua en ciberseguridad.
- **Infraestructura de servicios en la nube:** Modelos de infraestructura como servicio (IaaS) que proporcionan escalabilidad y flexibilidad ante las demandas del mercado.

La siguiente imagen, (1), proporciona información acerca de una representación visual clara de cómo se interrelacionan las diferentes infraestructuras dentro de una empresa y ayuda a identificar áreas donde pueden existir vulnerabilidades. La implementación de medidas de seguridad adecuadas en cada uno de estos componentes es esencial para proteger la integridad y la continuidad del negocio.

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

Imagen 1: Tipos de infraestructura



Autor: Gil (2024)

Fuente: Problemas en la adopción de modelos de gestión de servicios de tecnologías de información (2018)

Para toda empresa la infraestructura de red representa la herramienta fundamental para el manejo efectivo y eficiente de la información mediante los sistemas de apoyo. El éxito y competitividad están directamente relacionados con el correcto funcionamiento de la infraestructura tecnológica. Proaño y Col (2018) indican que los sistemas de información aseguran la transformación digital de las organizaciones. Por otro lado, Abrego y col (2019) indican que los sistemas de información y su infraestructura de apoyo influyen positivamente en el desempeño organizacional, mejorando la eficiencia interna, el control de costos y las ventas. Por su parte, Sánchez y col (2019) afirman que las empresas que invierten en mejorar la calidad de la seguridad de su infraestructura tecnológica tienden a obtener mejores resultados y

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

desempeño organizacionales. La economía y el mercado laboral actual demanda efectividad en el trabajo para asegurar la atención a los clientes, proveedores, socios, empleados y accionistas.

Desde el punto de vista técnico se pueden mencionar los elementos que conforman una infraestructura de red. Los dispositivos (routers, switches, firewalls), el cableado estructurado, la conectividad (tecnologías inalámbricas), sistemas de monitoreo y gestión, políticas de acceso y autenticidad, detección y prevención de intrusos.

Evolución de la infraestructura de red

La evolución tecnológica durante la última década ha sido vertiginosa, impulsada por la necesidad de una conectividad ubicua. Desde los inicios con mainframes y ARPANET, la red ha transicionado hacia infraestructuras basadas en TCP/IP en los años 90, hasta alcanzar la era actual dominada por la computación en la nube, el Internet de las Cosas (IoT) y la inteligencia artificial. Aspectos clave de esta evolución incluyen el incremento en la capacidad de transmisión (superando los 100 Gbps), la adopción masiva de redes inalámbricas flexibles y la consolidación de WANs seguras mediante tecnologías como MPLS y VPN.

Impacto de la vulnerabilidad de la infraestructura de redes en las empresas

Limones (2022) clasifica las vulnerabilidades más críticas en las organizaciones de la siguiente manera:

- **Vulnerabilidades digitales:** Incluyen errores de *software* (fallos de programación y falta de actualizaciones), configuraciones inseguras

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

(contraseñas débiles o servicios expuestos) y accesos no autorizados por controles deficientes.

- **Factor humano:** La falta de capacitación en ciberseguridad facilita ataques como el *phishing* y errores operativos.
- **Infraestructura física:** Riesgos derivados de desastres naturales, incendios o daños físicos a servidores y equipos críticos.
- **Dependencia externa:** La confianza en proveedores (nube o *software* de terceros) introduce riesgos si estos no cumplen estándares adecuados.
- **Sustracción de información:** La explotación de estas debilidades permite el robo de datos sensibles de usuarios y clientes.

La gestión de estas vulnerabilidades es indispensable para la continuidad del negocio. Complementariamente, un estudio de Kaspersky citado por Ciberseguridad Latam (2024) revela una realidad preocupante: cerca del 30% de las empresas experimenta fallas habituales de red, y el 49% identifica la detección y resolución de incidentes como su mayor desafío operativo. En cuanto al tiempo de recuperación tras una interrupción, el 74% de las organizaciones requiere entre 1 y 5 horas para restaurar el servicio, lo cual impacta directamente en la operatividad.

De este panorama se derivan repercusiones críticas para las empresas:

- **Impacto operativo y financiero:** Las interrupciones frecuentes causan mermas en la productividad y pérdidas financieras significativas por la inactividad de los sistemas.
- **Daño reputacional:** La percepción de inestabilidad afecta la confianza de clientes y socios comerciales.

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

- **Seguridad y presupuesto:** El compromiso de la integridad y confidencialidad de la información, sumado al incremento en los costos de mantenimiento correctivo, presiona los presupuestos organizacionales.

Ante estos desafíos, se reitera que la implementación de políticas de seguridad robustas, la capacitación continua del personal y la evaluación constante de riesgos son pilares fundamentales para proteger la infraestructura y asegurar la resiliencia empresarial.

Repercusiones en las empresas

Complementando el análisis de vulnerabilidades, Right Financial Crime Academy LLC (2024) categoriza las consecuencias del incumplimiento o fallo en la infraestructura de red en cuatro pilares críticos que afectan la sostenibilidad empresarial:

- **Repercusiones legales y regulatorias:** Incluyen la imposición de multas económicas y sanciones por incumplimiento de normativas de protección de datos, así como la responsabilidad civil ante terceros, lo cual puede derivar en litigios costosos. Asimismo, la dinámica legislativa obliga a una adaptación constante de los procesos internos para evitar brechas de cumplimiento.
- **Repercusiones organizacionales:** El impacto se refleja en el deterioro de la cultura y la moral laboral, exigiendo a menudo reestructuraciones forzadas y cambios operativos. Estas medidas correctivas suelen traducirse en gastos operativos adicionales que impactan negativamente en la rentabilidad.
- **Repercusiones reputacionales:** El daño a la imagen corporativa es, quizás, el efecto más difícil de revertir. La pérdida de confianza por parte de

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

clientes, proveedores y socios estratégicos disminuye la competitividad y la capacidad de la empresa para atraer talento y capital.

- **Repercusiones financieras:** Además de la disminución directa de ingresos por inactividad o fallas del servicio, se genera una carga financiera extra debido a los costos de remediación, litigios y la posible restricción en el acceso a nuevas fuentes de financiamiento.

Es importante destacar el impacto en la innovación: la excesiva preocupación por la inseguridad, nacida de infraestructuras vulnerables, actúa como una barrera. Esta aversión al riesgo limita la adopción de tecnologías emergentes, frenando la capacidad de la empresa para optimizar procesos y mantenerse competitiva en el mercado.

En consecuencia, el éxito a largo plazo de cualquier organización depende de su capacidad para trascender la reacción ante incidentes, adoptando estrategias proactivas de gestión de riesgos que integren la seguridad tecnológica como un pilar fundamental de la estrategia empresarial.

Metodología

El presente estudio se inscribe en un enfoque descriptivo-analítico. Su carácter descriptivo permite caracterizar la situación actual de las infraestructuras de red, mientras que su dimensión analítica profundiza en los factores de exposición al riesgo cibernético y en cómo estas vulnerabilidades condicionan la continuidad operativa del negocio.

La investigación adopta un paradigma mixto, integrando:

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

- Enfoque Cualitativo: Orientado a la evaluación heurística y al juicio de expertos para comprender la fenomenología de las amenazas en un entorno empresarial.
- Enfoque Cuantitativo: Proporciona el rigor necesario para cuantificar probabilidades de materialización de riesgos y medir las posibles consecuencias financieras mediante el análisis de datos.
- Revisión Documental: Se emplea como técnica de recolección de información, fundamentada en un análisis exhaustivo de literatura académica, informes técnicos y casos de estudio extraídos de bases de datos indexadas (IEEE, SCOPUS, Redalyc).

Ciclo de gestión de vulnerabilidades

El análisis se formaliza a través de un proceso estructurado de diez fases, constituyendo un ciclo de mejora continua:

1. Lanzamiento del Proyecto: Definición de objetivos, compromiso institucional y asignación de recursos tecnológicos.
2. Delimitación del Alcance: Definición técnica de los activos (hardware, software y datos) sujetos a evaluación.
3. Inventario de Activos: Registro técnico detallado (fabricante, versiones y configuraciones específicas).
4. Recolección de Información: Consulta de repositorios especializados (CVE, NVD) para identificar vulnerabilidades conocidas.
5. Evaluación y Priorización: Clasificación de los hallazgos según su nivel de criticidad e impacto potencial.
6. Análisis de Riesgo: Evaluación de la probabilidad de explotación frente a la relevancia del activo.

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

7. Desarrollo del Plan de Mitigación: Diseño de estrategias correctivas, incluyendo actualizaciones, cambios de configuración o controles compensatorios.
8. Implementación: Ejecución de medidas bajo protocolos de gestión de cambios para minimizar la afectación operativa.
9. Seguimiento y Verificación: Validación mediante escaneos de seguridad y auditorías posteriores.
10. Documentación y Lecciones Aprendidas: Sistematización de los resultados para la retroalimentación del sistema de gestión de seguridad.

Este modelo cíclico permite que las organizaciones evolucionen de un enfoque reactivo a uno proactivo, fortaleciendo la resiliencia tecnológica frente a un panorama de amenazas en constante transformación.

Recomendaciones para el correcto funcionamiento de la infraestructura de red en una empresa

Para garantizar una infraestructura robusta, escalable y segura, las organizaciones deben adoptar un enfoque integral que armonice el *hardware*, la gestión y la ciberseguridad. Las recomendaciones clave se agrupan en cuatro ejes estratégicos:

- **Arquitectura de Dispositivos y Conectividad:** La base operativa requiere el despliegue de *routers* y *switches* gestionables que permitan un control granular del tráfico. Es fundamental complementar esto con cableado estructurado certificado y redes inalámbricas corporativas protegidas mediante protocolos de cifrado robustos, garantizando así un rendimiento estable y una movilidad segura.

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

- **Gestión Centralizada y Monitoreo Proactivo:** La administración debe apoyarse en consolas centralizadas que permitan la visibilidad total de la red. Herramientas de monitoreo (como PRTG Network Monitor) son indispensables para la supervisión en tiempo real del desempeño, la disponibilidad y la detección de anomalías, facilitando la toma de decisiones basada en datos.
- **Continuidad Operativa y Redundancia:** La resiliencia se construye mediante la prevención de puntos únicos de falla. Esto incluye la implementación de enlaces redundantes para asegurar el tráfico en caso de caída de proveedores y el uso de Sistemas de Alimentación Ininterrumpida (SAI) para proteger los equipos críticos ante fluctuaciones o cortes eléctricos.
- **Estrategias de Ciberseguridad (Defensa en Profundidad):** Más allá del *firewall* perimetral, la seguridad debe incluir:
    - **Control de Acceso:** Políticas de autenticación multifactor y segmentación de red.
    - **Detección Activa:** Despliegue de sistemas de detección y prevención de intrusos (IDS/IPS) capaces de identificar patrones de ataque en el tráfico interno y externo.

La convergencia de estos elementos permite a la organización transitar hacia una infraestructura confiable, capaz no solo de soportar las demandas operativas actuales, sino de adaptarse proactivamente ante la evolución constante de las amenazas cibernéticas.

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

Discusión

El estudio de las vulnerabilidades en la infraestructura de red es hoy un imperativo estratégico, dado que las ciberamenazas evolucionan en sofisticación y frecuencia. La implementación de análisis sistemáticos permite a las organizaciones identificar y neutralizar brechas de seguridad antes de su explotación, salvaguardando así sus activos críticos y garantizando la continuidad operativa.

Más allá de la protección técnica, este análisis es un pilar fundamental para el cumplimiento de normativas de protección de datos. Al demostrar una gestión proactiva de la seguridad, las empresas no solo mitigan riesgos, sino que fortalecen la confianza de clientes y socios estratégicos, posicionando la ciberseguridad como un valor añadido en su reputación corporativa.

Sin embargo, la ciberseguridad debe entenderse como un proceso iterativo de mejora continua y no como un esfuerzo aislado. La realización periódica de estos análisis fomenta una cultura organizacional resiliente, capaz de adaptarse dinámicamente a nuevas amenazas.

A pesar de estos beneficios, las organizaciones enfrentan desafíos estructurales significativos, como la limitación de recursos especializados y la creciente complejidad de entornos tecnológicos heterogéneos, que dificultan la priorización efectiva de los riesgos. Por lo tanto, es indispensable que las empresas desarrollen estrategias de gestión claras, que integren herramientas automatizadas con políticas organizacionales sólidas, permitiendo una respuesta ágil y eficiente ante un panorama digital en constante cambio.

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

Conclusiones

La infraestructura de red de una empresa es un conjunto integral de componentes que deben trabajar en conjunto para garantizar la eficiencia y la seguridad en la comunicación de los dispositivos y sistemas de apoyo a la gestión de trabajo. Las infraestructuras de redes para las empresas traen innumerables beneficios: mejora en la productividad, facilitan el acceso a la información, se orientan hacia la seguridad y hacia la protección de los datos, permiten la implementación de soluciones tecnológicas avanzadas, una eficiente infraestructura permite a las empresas adaptarse rápidamente a cambios en el mercado, innovar en sus procesos y ofrecer mejores servicios a sus clientes.

Todos los beneficios de una infraestructura de red pueden verse opacados por fallas en su seguridad. Estas fallas pueden tener diversas causas desde vulnerabilidades técnicas, pasando por errores humanos hasta ataques cibernéticos. Para cualquier empresa las consecuencias pueden estar referidas a interrupciones en los servicios, incumplimiento de compromisos financieros, pérdidas de datos, pérdida de datos sensibles de clientes o de usuarios, desprestigio, pérdida de la imagen. A su vez, estas consecuencias pueden tener repercusiones económicas representativas.

Las organizaciones deben estar en evaluación continua de riesgos, implementar medidas de seguridad aprovechando todos los beneficios y recursos tecnológicos, capacitas a su personal para trabajar en función de la seguridad, actualizar sistemas y tecnología en general y tener planes de respuesta a contingencias.

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

Referencias

Abrego D, Medina J y Sánchez M. (2019) **Los sistemas de información en el desempeño organizacional: un marco de factores relevantes**. Revista Investigación administrativa. Volumen 44. Número 115. Disponible: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-76782015000100001 [Consulta, noviembre, 2024]

Castro, M. F., Orellana Contreras, S. Y., y Martillo Pazmiño, I. O. (2018). **Los sistemas de información y su importancia en la transformación digital de la empresa actual**. Revista Espacios. Disponible: https://www.revistaespacios.com/a18v39n45/a18v39n45p03.pdf [Consulta, noviembre, 2024]

Ciberseguridad Latam (2024). **Problemas de red afectan a casi la mitad de las empresas industriales**. Disponible: https://ciberseguridadlatam.com/problemas-de-red-afectan-a-casi-la-mitad-de-las-empresas-industriales/ [Consulta, noviembre, 2024]

Limones, E. (2022). **Análisis de vulnerabilidades informáticas** [Blog]. OpenWebinars.net. https://openwebinars.net/blog/analisis-de-vulnerabilidades-informaticas/ [Consulta, noviembre, 2024]

Martínez D (2024). **La evolución de las redes de datos. Del pasado al presente**. Disponible: https://cultura-brillante.com/la-evolucion-de-las-redes-de-datos-del-pasado-al-presente/?expand_article=1 [Consulta, noviembre, 2024]

Melendez-, K y. Dávila-R, (2018) "**Problemas en la adopción de modelos de gestión de servicios de tecnologías de información. Una revisión sistemática de la literatura**", DYNA, vol. 85, no. 204, pp. 215-222, Ene. Disponible: https://doi.org/10.15446/dyna.v85n204.57076 [Consulta, noviembre, 2024]

Molina, Y., & Orozco, L. G. (2020). **Vulnerabilidades de los Sistemas de Información: Una revisión**. Disponible: https://dspace.tdea.edu.co/handle/tdea/1398 [Consulta, noviembre, 2024]

Right Financial Crime Academy LLC (2024), **Comprender las consecuencias del incumplimiento: riesgos y sanciones**. Disponible en: https://financialcrimeacademy.org/es/consecuencias-del-incumplimiento-las-importantes-consecuencias-del-incumplimiento/ [Consulta, noviembre, 2024]

Nro. Depósito Legal
AR2022000073
Nro. ISNN 2957-6814

Rojas, R (2024) A**daptación continua: La evolución de la infraestructura de TI**. Icorp.com. Disponible: https://icorp.com.mx/blog/evolucion-de-la-infraestructura-de-ti/ [Consulta, noviembre, 2024]

Sánchez D, Tovar M y Quintero M (2019). **Influencia de la seguridad en los sistemas y en la infraestructura de red**. Disponible: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0186-10422017000200303 [Consulta, noviembre, 2024]

Schneier, B. (2015**). Applied Cryptography: Protocols, Algorithms, and Source Code in C**. John Wiley & Sons. Disponible: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119183471 [Consulta, noviembre, 2024]