

La importancia de la auditoría de sistemas en el comercio electrónico

Camilo Hernán Umaña Martínez ¹

Resumen

El artículo describe de una forma muy general la importancia y los beneficios de realizar una auditoría de sistemas al comercio electrónico, el cual está expuesto a nuevos riesgos que afectan a las organizaciones que optaron por adaptarse al sistema, esto permitiendo que los ciberdelincuentes generen diferentes métodos de fraude y beneficiarse de las vulnerabilidades, al detectar estos riesgos se alerta a las organizaciones con recomendaciones que pueden implementar para aumentar su seguridad, se explica como la norma ISO 19011:2018 directrices para la auditoría de los sistemas de gestión permite al auditor de sistemas realizar una auditoría de forma eficiente de acuerdo con sus principios, capacidades y requerimientos necesarios para realizarla, el artículo también resalta el crecimiento que ha tenido el comercio electrónico en Colombia en los últimos años y las regulaciones que actualmente lo rige, se explica que la auditoría de sistemas es una herramienta que se utiliza para ayudar al comercio electrónico evaluando los riesgos y controles que hacen parte de los sistemas de información y como al realizar estas evaluaciones surgen recomendaciones para mejorar la seguridad, cumplimiento normativo, desempeño y confianza a los usuarios.

¹Camilo Hernán Umaña Martínez, profesional de administración de empresa egresado de la universidad Antonio Nariño de Bogotá D, c, Estudiante de la especialización de auditoría de sistemas de la universidad Antonio Nariño, cumana41@uan.edu.co

Palabras claves: Auditoría de sistemas, Comercio electrónico, Riesgo, Normas, importancia, Regulación

Abstract

The article describes in a very general way the importance and benefits of carrying out a systems audit of e-commerce, which is exposed to new risks that affect organizations that chose to adapt to the system, this allowing cybercriminals to generate different methods of fraud and benefit from vulnerabilities, when these risks are detected, organizations are alerted with recommendations that they can implement to increase their security, It is explained how the ISO 19011:2018 guidelines for the audit of management systems allows the systems auditor to carry out an audit efficiently according to its principles, capabilities and requirements necessary to perform it, the article also highlights the growth that e-commerce has had in Colombia in recent years and the regulations that currently govern it, It is explained that systems auditing is a tool that is used to help e-commerce by evaluating the risks and controls that are part of information systems and how when carrying out these evaluations, recommendations arise to improve security, regulatory compliance, performance and user confidence.

Keywords: Systems audit, E-commerce, Risk, Standards, importance, Regulation

Introducción

Los avances tecnológicos son una parte fundamental para el desarrollo de la humanidad y el avance de las organizaciones, mejorando la calidad de vida. Estos avances obligan a las empresas a adaptarse al mercado competitivo, al surgir estas

innovaciones tecnológicas se manifiestan nuevos riesgos debido a que son nuevos y desconocidos lo cual puede generar que personas o situaciones externas e internas busquen la manera de encontrar vulnerabilidades para poder cometer crímenes y poder obtener un beneficio propio.

El comercio electrónico ha permitido que los usuarios tengan acceso a los productos y servicios de forma rápida y fácil, pero aumenta el riesgo de exposición de su información sensible. Si la organización, no cumple con los reglamentos y los protocolos de seguridad necesarios aumenta los riesgos, las organizaciones en Colombia buscan anticiparse a los posibles riesgos que se puedan generar en un futuro y realizar planes para proteger la información de los usuarios. De acuerdo con (Ramírez, E. 2022) en su trabajo de investigación afirma que “El comercio electrónico trae consigo muchos riesgos que paralizan a un cliente potencial a llevar a cabo su compra, como puede ser el robo de datos a particulares y empresas cuando se realiza algún tipo de transacción online”

Según el (MINTIC, 2023, p. 15) en su guía afirma que la auditoría de sistemas “Es aquella actividad donde se evalúa el manejo y la protección de la información residente en los sistemas de información, también califica la aptitud del recurso humano que gestiona estas plataformas y la eficiencia del recurso informático” por lo tanto la auditoría de sistemas cumple un rol muy importante en el comercio electrónico ya que por medio de expertos que cuentan con conocimientos y habilidades desarrolladas les permite evaluar la gestión de riesgos realizada al comercio electrónico de la organización y presentar las debidas recomendaciones a las empresas para que tomen su opinión de las posibles mejoras que puede realizar para aumentar su seguridad y la

confianza de los usuarios evitando de esta manera fraudes, robos de información, suplantaciones y demás riesgos que pueden afectar a la integridad de la organización.

El presente artículo se enfocará en la importancia de realizar auditoría de sistemas en el comercio electrónico evaluando diferentes factores de riesgo en las que está expuesta la organización y enfocándose en el reglamento colombiano que regula el comercio electrónico y la protección de la información de los usuarios.

Por lo tanto, este artículo se enfocará realizando una pregunta fundamental qué es ¿cuál es la importancia de realizar una auditoría de sistemas al comercio electrónico?

Metodología

Para identificar la importancia de la auditoría de sistemas en el comercio electrónico se realizará una investigación bibliográfica. Para esto se realizará la búsqueda con palabras claves como: (auditoría de sistemas, riesgos, comercio electrónico, aportes, importancia) se tendrán en cuenta artículos con más o menos de 5 años de antigüedad y las leyes y reglamentos que regulan el comercio electrónico, se llevará a cabo una investigación cuantitativa de casos en los cuales se evidencie los fraudes, riesgos y vulnerabilidades que se presentan en el comercio electrónico con esta información se responderá la pregunta de la investigación, los motores de búsqueda que se utilizarán serán Google académico, biblioteca Antonio Nariño.

La información recolectada buscará determinar la importancia que tiene realizar una auditoría de sistemas al comercio electrónico en la actualidad, por ende, se realizará una investigación de noticias, estadísticas, estudios realizados, tesis, revistas y artículos

que permitan el desarrollo de los objetivos de la investigación y páginas webs confiables que contengan información clave relacionada con la investigación.

Resultados.

Comercio electrónico

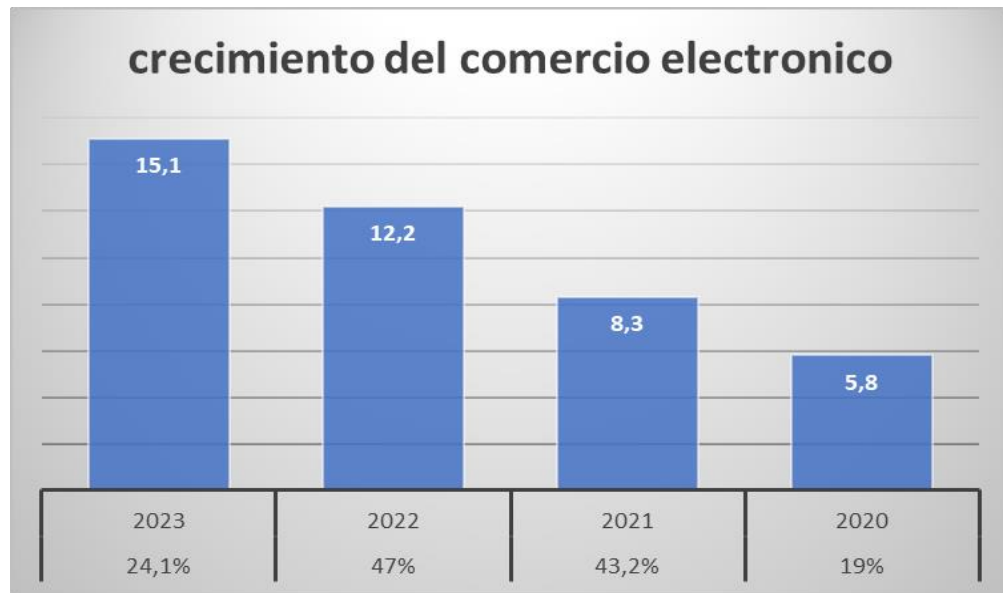
De acuerdo con (Mejía, J. 2023, p. 48). En su libro *negocios electrónicos*, el comercio electrónico se define como “transacciones comerciales con capacidad digital entre organizaciones o individuos” por ende, para realizar este tipo de transacciones se requiere el intercambio de información tanto de la organización la cual suministra su ubicación, opciones de pago como números de cuenta y características del producto o servicio y por parte del comprador información personal, como nombre completo, número de identificación, dirección, correo electrónico, número de contacto y método de pago como tarjetas de crédito, dependiendo del tipo de producto que se va a adquirir o el tipo de cliente que puede ser persona natural o jurídica.

El incremento del comercio electrónico en Colombia en los últimos años de acuerdo con la cámara colombiana de comercio electrónico:

Según la (cámara colombiana de comercio electrónico, 2023). En su informe describe que: el total de ventas en línea para el primer trimestre de 2023 fue aproximadamente de COP 15,1 billones, lo que se traduce en un aumento del 24,1 % respecto al primer trimestre de 2022 y de un 83,2 % respecto al mismo trimestre de 2021. Cabe aclarar que respecto al trimestre anterior (cuarto trimestre de 2022) las ventas disminuyeron 1,9 % lo que es un comportamiento típico pues el último trimestre del año se caracteriza por el alto consumo.

Tal como se representa en la figura N°1. El incremento que se obtuvo fue gracias a las nuevas tecnologías y al poder de adaptación de las empresas ya que se adecuaron a las situaciones y requerimientos que los clientes necesitaban, otra de las situaciones por las que el comercio electrónico incremento fue por la pandemia lo que aumento que las personas realizaran las compras en línea ya que al realizarlas físicamente aumentaba el riesgo de contagio por el virus que en ese momento afectaba significativamente la salud de las personas a nivel mundial, el comercio electrónico creció de la siguiente manera:

Figura 1 Número de transacciones aprobadas de las ventas en línea



Fuente: Elaboración propia

Regulación al comercio electrónico

La información ha sido una parte importante para el comercio electrónico, pero en la década de los noventa no se le daba la misma importancia a los documentos electrónicos como los físicos al observar esta problemática la comisión de las naciones unidas para el derecho mercantil internacional (CNUDMI) diseñó una ley en 1996

llamada ley modelo sobre el comercio electrónico la cual tiene como finalidad lo siguiente: “posibilitar y facilitar el comercio por medios electrónicos ofreciendo a los legisladores un conjunto de reglas internacionalmente aceptables encaminadas a suprimir los obstáculos jurídicos y a dar una mayor previsibilidad al comercio electrónico” Por lo tanto, el objetivo de la regulación es buscar lo siguiente:

- Protección al consumidor para que no se presenten situaciones de fraudes o engaños.
- Protección de datos en la cual se debe informar con anticipación
- manejo que se le va a dar a este tipo de información

Riesgo en el comercio electrónico

De acuerdo (Campos, A. Castañeda, R. & Holguín, F, 2020, P. 63). En su libro *auditoria de estados financieros y su documentacion con énfasis en riesgos* se define el riesgo como la “posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra perjuicio o daño” por lo tanto el riesgo se puede entender como la probabilidad de que ocurra un hecho no esperado en el cual se generen situaciones negativas, en el comercio electrónico se pueden presentar diferentes riesgos los cuales pueden generar afectaciones tanto a los consumidores como a los comerciantes. Según la (cámara colombiana de comercio electrónico, 2023). En su artículo *Estos son los tres tipos de fraudes que generan mayor afectacion a los e-commerce en colombia según ClearSale* refiere que de acuerdo con los análisis realizados a las bases de datos por la ClearSale quiere dar a conocer los fraudes más comunes que se presentaron en el último periodo y que de esta manera se puedan realizar medidas de prevención y protección en los negocios electrónicos.

Fraude de principiante con tarjeta en mano: consiste en la venta o robo de tarjetas de crédito o débito con la cual se realizan compras antes de que el propietario pueda realizar el bloqueo de la tarjeta

Fraude amigo: consiste en que el propietario (estafador) realiza compras y realiza el pago con tarjeta de crédito/débito u otro medio de pago digital y después de recibir el producto realiza la reclamación de la devolución del dinero en la que afirma que no recibió el producto, no realizó la compra o que realizó la devolución del producto por tal motivo se realiza un reembolso del dinero.

Fraudes profesionales con bases de datos: se refiere cuando el hacker realiza el robo de una base de datos en la que se encuentre datos confidenciales con información precisa de las cuentas de diferentes clientes esto puede pasar desapercibido al realizar una compra, este tipo de bases de datos se venden en la internet oscura y el comprador realiza pequeñas compras hasta realizar la mayor cantidad de transacciones.

La suplantación es otro de los riesgos a los que está expuesto el comercio electrónico de acuerdo con (Arbeláez, M. F. 2021, April 5). El periódico el tiempo en su artículo: *Así están suplantando sitios web de comercio electrónico* detalla el caso de Luis quien realizó una compra por un sitio web parecido a mercado libre y que contaba con características similares a la página web oficial, como el enlace, candado de seguridad y menú de selección de productos, por lo cual no genero ningún tipo de sospecha y procedió a contactarse con el vendedor (estafador) quien le informo el método de pago, Luis realizó el pago pero no obtuvo ninguna información del envío del producto lo que generó sospecha e intentó comunicarse con el vendedor pero ya no respondía, esta modalidad que realizan es muy frecuente para estafar a la mayor

cantidad de personas ya que al observar que el sitio está certificado no genera sospecha y puede generar el robo de información de las tarjetas de crédito o de la información confidencial de los que ingresan a este tipo de sitios.

Así como en el caso anterior uno de los riesgos que presentan en el comercio electrónico es el acceso a la privacidad de los datos de los clientes, de acuerdo con la (superintendencia de industria y comercio, 2019). En su *guia sobre el tratamieto de datos personales* afirma que “Las empresas deberían proteger los datos personales del consumidor, asegurándose de que sus prácticas relacionadas con la recopilación y el uso de datos del consumidor sean legales, transparentes y justas” con esto podemos concluir que al realizar una transacción electrónica y el cliente suministra sus datos personales las empresas tienen el deber de realizar y tener los debidos procesos y protocolos de seguridad para resguardar esta información y que no llegue al poder de personas externas generando fraudes.

Otros tipos de riesgo de acuerdo con la revista (Semana, 2023) el informe realizado por Sonicwall llamado *amenazas cibernéticas 2023* “Colombia se encuentra en el listado de los 10 países del mundo con más ataques de “ransomware” o robo de información en 2022”, pero uno de los riesgos cibernéticos que se presentan es el “pushing” estos cuentan con las siguientes características como se muestra en la tabla

N° 1

Tabla 1 Descripción de riesgos Ransomware y Pushing

Riesgos	Descripción
Ransomware	<ul style="list-style-type: none"> ● Robo de contraseñas y usuarios ● Robo de número de tarjetas de crédito ● Realizar transacciones y vaciar cuentas bancarias ● Suplantación de identidad para realizar compras ● Venta de información en el mercado negro
Pushing	<ul style="list-style-type: none"> ● Suplantación de identidad de las empresas ● Estafa y robo por medio de: mensajes de texto y correo electrónico

Fuente: Elaboración propia

Debido a los riesgos que se mencionaron anteriormente la (cámara colombiana de comercio electrónico, 2023). En su artículo *Prevenga los ciberataques en los ecommerce* recomienda usar las siguientes medidas de seguridad en el comercio electrónico para proteger los datos del usuario:

utilizar un protocolo de seguro de transferencia de hipertexto: para ayudar a la protección de los datos de los usuarios permitirá cifrar los datos enviados y evitar que sean obstruidos por ciberdelincuentes

obtener un certificado digital SSL: permite aumentar la confianza del cliente y encriptar los datos que se utilizan entre el sitio web y el navegador del usuario

instalar programas antimalware: Ya que los escáneres de programa maligno permiten la búsqueda de software malicioso y protegen las cuentas de los usuarios. Es

recomendable actualizar regularmente el software, incluyendo el sistema operativo, administrativo y el navegador web.

Usar un firewall o dispositivo de seguridad de red: Con el fin de proteger el sitio web contra accesos no autorizados y bloquear tráfico no deseado, como escaneos de puertos y ataques de denegación de servicio, se implementan medidas de seguridad.

Implementar políticas de contraseñas seguras: se recomienda la renovación de las contraseñas en tiempos determinados para aumentar la seguridad

Realizar copias de seguridad periódicas de datos en una ubicación segura: se recomienda realizar copias de seguridad en servidores de terceros que permitan aumentar su seguridad y para eventualidades realizar con anterioridad backup de forma segura

Contar con una pasarela de pago segura: Es necesario tener un proveedor de servicios de comercio electrónico que también proporcione un enlace de pago segura, para garantizará la protección de los datos de los clientes mediante el uso de encriptación y otras medidas de seguridad.

Auditoría de sistemas

De acuerdo con (Nuño, P. 2023, August 9). En su artículo describe que “La auditoría de sistemas supone la revisión y evaluación de los controles y sistemas de informática, así como su utilización, eficiencia y seguridad en la empresa, la cual procesa la información”. Por lo tanto, la auditoría de sistemas es una herramienta que permite a las empresas mejorar su desempeño evaluando los diferentes aspectos de la organización que tengan relación con los sistemas de tecnología e información, y de acuerdo con los hallazgos recolectados con el fin de identificar si la organización está

realizando los procesos correctamente, cumpliendo con los protocolos de seguridad y con las distintas normas establecidas tanto internamente como externamente.

La norma ISO 19011:2018 directrices para la auditoría de los sistemas de gestión es un documento el cual permite orientar a quien necesite realizar una auditoría de sistemas como se observa en la figura N°2, de acuerdo con esta norma para realizar una auditoría de sistemas y asegurar que se realice con transparencia y de forma efectiva se debe contar con los siguientes principios.

Principios

Integridad: el auditor debe ser consciente de sus capacidades para aceptar el tipo de auditoría que se realizará, debe ser una persona con ética y honesta la cual no se deje influencia por personas internas o externas que puedan alterar su opinión y siempre actuar de forma justa de acuerdo con su criterio

Presentación imparcial: los resultados de la investigación deben ser completamente exactos y no se debe realizar ningún tipo de omisión en los resultados encontrados, se debe especificar con detenimiento los pros y contras de la auditoría realizada de forma clara

Cuidado profesional: el auditor debe actuar con profesionalismo y que su participación sea acorde con el nivel de importancia que se le da, ya que el auditado deposita toda su confianza en él, por lo tanto, la auditoría debe ser realizada rigurosamente y con mucho cuidado

Confidencialidad: el auditor tiene acceso a información confidencial por lo tanto esta debe ser protegida y actuar con discreción, y no debe ser usada para beneficio del auditor, el auditado o de terceros

Independencia: el auditor debe ser independiente y no puede afectar su criterio el cual debe ser de forma imparcial y su opinión solo puede estar basada en los hallazgos y resultados encontrados

Enfoque basado en la evidencia: el auditor deberá enfocar la auditoría solo en la información disponible y que esta sea verídica la cual pueda cerciorarse por medio de muestreos en los tiempos y con los recursos disponibles.

Enfoque basado en el riesgo: la auditoría debe basarse en las necesidades que el cliente requiera enfocándose en los riesgos detectados y las oportunidades que influyen en la planificación y la presentación de informes.

Figura 2 Realización de una auditoría



Fuente: Elaboración propia

¿Cuál es la importancia de realizar una auditoría de sistemas al comercio electrónico?

Realizar una auditoría de sistemas a comercio electrónico es fundamental ya que está expuesto a diferentes riesgos y maneja información importante como los son: transacciones realizadas, datos de tarjetas de crédito y personales, entre otras, Los clientes al realizar este tipo de compras depositan la confianza de sus datos sensibles a las organizaciones y el uso inadecuado de esta información puede ser utilizada de manera fraudulenta y si una organización no cuenta con los controles correctos puede facilitar el acceso de ciberdelincuentes a esta información, una organización tiene la responsabilidad de proteger los datos de sus clientes y al realizar una auditoría de sistemas aumenta la confianza de los clientes generando un grado de seguridad de que la organización se preocupa por la protección de sus datos, y permitiendo mejorar los procesos, realizando la evaluación de riesgos y controles e identificar si se está efectuando el cumplimiento normativo.

Así mismo los riesgos se encuentran en entornos internos y externos por lo tanto deben ser evaluados, debido a que los empleados de la organización podrían manipular la información, comercializar y cometer fraudes. Una auditoría al comercio electrónico genera confianza al garantizar que se tendrá en cuenta la información que se pueda verificar evitando así posibles alteraciones y resultados incorrectos, con los conocimientos del auditor líder y de su equipo especializado se realiza a detenimiento el paso a paso de la auditoría de sistemas enfocándose en los criterios y necesidades del

cliente con profesionalismo, actuando siempre con honestidad, discreción y su criterio no será influenciado por terceros, evitando siempre la filtración de información.

Al finalizar la auditoría el auditor de acuerdo con su criterio realiza recomendaciones para mejorar el desempeño de procesos que se realizan en el comercio electrónico, este tipo de recomendaciones pueden ayudar a la organización a tomar medidas correctivas para mitigar los riesgos y evitar posibles amenazas en un futuro, al realizar este tipo de acciones correctivas permite mejorar el desempeño y protección de la organización.

De acuerdo con (AdminACTI, 2019) en su artículo la auditoría de sistemas se describe como “proceso de revisión de los sistemas de información (SI) y tecnologías de la información (TI) que ayuda a las empresas a identificar hallazgos, mitigar riesgos e implementar controles adecuados que permitan proteger su información crítica y valiosa”. Por ende, una auditoría de sistemas preventiva en el comercio electrónico puede ofrecer aportes y beneficios como los que se reflejan en la figura N°3. Para mejorar el desempeño y evitar que sea vulnerada la información al realizar a tiempo las medidas correctivas por parte de la organización, como expresa (Carrión. N, 2023). *La importancia de la Auditoría de Sistemas en la era digital* en su artículo nos describe los siguientes ejemplos en los cuales resalta la importancia de realizar una auditoría de sistemas en la actualidad.

Figura 3 Aportes de auditoría de sistemas al comercio electrónico



Fuente: Elaboración propia

Identificación precisa de vulnerabilidades: los auditores con el uso de diferentes herramientas realizan diversos tipos de evaluaciones y análisis para determinar las vulnerabilidades que se pueden encontrar en los sistemas y detectar esos puntos débiles y realizar recomendaciones que permitan mitigar los riesgos generando protección a los sistemas de seguridad

Cumplimiento normativo y mejores prácticas: la auditoría se encarga de que las políticas de la organización y las normas se formen para no incurrir en una falta grave debido a que actualmente se regula cada vez más el cumplimiento del tratamiento, protección y uso de datos personales o información de la organización.

Detección temprana y respuesta rápidas: la auditoría de sistemas se encarga de detectar anomalías como accesos no autorizados, ataques cibernéticos y amenazas que puedan afectar a los sistemas, realizar una detección temprana permite

actuar de manera rápida y mitigar el impacto que puede causar minimizando el riesgo de que se pueda repetir o prevenir un ataque al sistema.

Optimización de procesos y recursos: Al realizar una auditoría se pueden identificar áreas las cuales requieren una mejora, el auditor puede utilizar diferentes métodos y herramientas como la observación, listas de chequeo, entrevistas entre otros que permitan analizar las áreas que requieran un mejoramiento y poder optimizar los procesos de la organización con soluciones innovadoras aumentando la productividad, mitigar riesgos y reducción de precios.

Fortalecimiento de confianza: Al realizar una auditoría de sistemas se evalúan factores como la seguridad que buscan mejorar constantemente para generar confianza tanto a sus clientes como a sus socios para demostrar que la organización está comprometida con la protección de su privacidad y del cuidado de su información y con el cumplimiento normativo.

Conclusiones

De acuerdo con lo anterior se puede identificar que, realizar una auditoría de sistemas al comercio electrónico en una era digital como la actual es de vital importancia, ya que permite proteger un de los recursos más valioso que es la información e incluso la cámara de comercio realiza unas recomendaciones para la protección de los datos de los usuarios los cuales deben ser evaluados debido a que son temas relacionados con seguridad de contraseñas, actualizaciones de software, accesos no autorizados, actualizaciones de sistemas, los cuales pueden mejorar su desempeño y seguridad en la organización evitando el acceso a ciberdelincuentes, es importante tener

en cuenta la norma ISO 19011:2018 Directrices para la auditoría de los sistemas de gestión al realizar una auditoría ya que permite que con sus directrices como lo son los: principios y lineamientos para realizar una auditoría de sistemas correctamente, permitiendo así la evaluación y revisión de los riesgos y controles de los sistemas de la organización que puede verse afectada por factores internos o externos, y debido al crecimiento progresivo del comercio electrónico el cual debe cumplir con las regulaciones y normas actuales es esencial efectuar una auditoría de sistemas que tiene como objetivo mejorar el desempeño de la organización como: optimización de procesos, seguridad, confianza y cumplimiento normativo nacional e internacional aumentando la posibilidad de realizar medidas correctivas de una organización de forma oportuna y poder intervenir en los nuevos riesgos y métodos de ciberdelincuentes que buscan un beneficio propio al querer apoderarse de la información y afectada la organización.

Referencias

- MINTIC. (2023). Guía de Auditoría. Obtenido de seguridad y privacidad de la información: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf
- Ramírez, E. (2022). Plan de marketing digital de petburush: creación e implementación del e-commerce a través del modelo de negocio dropshipping. Obtenido de universidad de cádiz: https://rodin.uca.es/bitstream/handle/10498/28984/Ram%C3%ADrezSalado_Esteban_TFM_2022.pdf?sequence=1&isAllowed=y
- Mejía Trejo, J. (2023). Negocios electrónicos: una descripción de sus principales herramientas. 1. Academia Mexicana de Investigación y Docencia en Innovación (AMIDI). <https://elibro-net.ezproxy.uan.edu.co/es/ereader/bibliouan/228012>
- Camara colombiana de comercio electrónico. (2023). Informe trimestral del comportamiento del comercio electrónico en Colombia. <https://ccce.org.co/wp-content/uploads/2017/06/1Q-INFORME-TRIMESTRAL-DEL-COMERCIO-CCCE-1.pdf>
- Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996) con su nuevo artículo 5 bis aprobado en 1998 | Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. (n.d.). https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_commerce
- Ley 527 de 1999 - Gestor Normativo. (n.d.). Función Pública. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276>
- Campos, A. Castañeda, R. & Holguín, F. (2020). Auditoría de estados financieros y su documentación - Google Books”) Instituto Mexicano de Contadores Públicos. <https://elibro-net.ezproxy.uan.edu.co/es/ereader/bibliouan/151231>
- Camara Colombiana De Comercio Electrónico. (2023). Estos son los tres tipos de fraudes que generan mayor afectación a los e-commerce en Colombia según ClearSale.. <https://www.ccce.org.co/noticias/estos-son-los-tres-tipos-de-fraudes-que-generan-mayor-afectacion-a-los-e-commerce-en-colombia-segun-clearsale/>
- Arbeláez, M. F. (2021, April 5). Así están suplantando sitios web de comercio electrónico. El Tiempo. <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/tacticas-de-suplantacion-de-sitios-web-de-comercio-electronico-578204>
- Superintendencia de industria y comercio. (2019). Guía sobre el tratamiento de datos personales para fines de comercio electrónico [https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico\(1\).pdf](https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico(1).pdf)

- semana. (01 de agosto de 2023). ¿Por qué Colombia está entre los países con mayor robo o secuestro de datos? Obtenido de <https://www.semana.com/hablan-las-marcas/articulo/por-que-colombia-esta-entre-los-paises-con-mayor-robo-o-secuestro-de-datos/202330/>
- Nuño, P. (2023, August 9). Auditoría de sistemas. Emprendepyme. <https://emprendepyme.net/auditoria-de-sistemas.htm>
- ISO 19011:2018. (2018). Directrices para la auditoría de los sistemas de gestión. PDF. <https://www.cecep.edu.co/documentos/calidad/norma-iso-19011-2018.pdf>
- adminACTI. (2019). La Importancia de la Auditoría de Sistemas – AudiConsultI. <https://www.audiconsulti.com/importancia-de-la-auditoria-de-sistemas/>
- Carrión, N. M. (12 de mayo de 2023). linkedin. Obtenido de la importancia de la auditoría de sistemas en la era digital : <https://www.linkedin.com/pulse/la-importancia-de-auditor%C3%ADa-sistemas-en-era-digital-nora/?originalSubdomain=es>
- camara colombiana de comercio electronico. (25 de agosto de 2023). prevenga los ciberataques en los ecommerce: <https://www.ccce.org.co/noticias/prevenga-los-ciberataques-en-los-ecommerce-2/>