Revista de investigación de sistemas e informática
16(2): 169-176 (2023)
DOI: https://doi.org/10.15381/risi.v16i2.27141

ISSN: 1815-0268 (Impreso) / ISSN: 1816-3823 (Electrónico)
Facultad de Ingeniería de Sistemas e Informática - UNMSM

La seguridad de la información en la gestión de continuidad del negocio en América Latina

Information security in business continuity management in Latin America

Renato Pedro Guerra Garib
https://orcid.org/0000-0003-3488-8485
renato.guerra @unmsm.edu.pe

Manuel Fernando Pumasunco Rivera
https://orcid.org/0000-0002-4394-8526
manuel.pumasunco@unmsm.edu.pe

Candy Esther Seminario Sánchez
https://orcid.org/0000-0002-5918-7813
candy.seminario@unmsm.edu.pe

Universidad Nacional Mayor de San Marcos, Lima, Perú

Recibido: 19/09/2023 - Aceptado: 15/10/2023 - Publicado: 30/12/2023

RESUMEN

En los últimos cinco años se han incrementado los incidentes de ciberseguridad en América Latina, impactando desfavorablemente en la continuidad del negocio de muchas empresas. Este problema es un desafío para la nueva gestión empresarial y es motivo de la presente investigación, cuyo objetivo es lograr la continuidad del negocio a través de la seguridad de la información. El método utilizado es exploratorio y el diseño es no experimental. En la investigación se realizó un diagnóstico tomando como referencia "Los aspectos de seguridad de la información en la gestión de continuidad del negocio", investigación realizada por la Comisión Económica para América Latina y el Caribe (CEPAL). Los resultados reflejan que no necesariamente una empresa u organización que cuente con una certificación ISO 27001 de Seguridad de la Información, tiene garantizada la continuidad de su negocio.

Palabras clave: Seguridad de información, continuidad de negocio, ciberseguridad, globalización.

ABSTRACT

In the last five years, cybersecurity incidents have increased in Latin America, unfavorably impacting the business continuity of many companies. This problem is a challenge for new business management and is the reason for this research, whose objective is to achieve business continuity through information security. The method used is exploratory and the design is non-experimental. In the investigation, a diagnosis was carried out taking as reference "The aspects of information security in business continuity management", research carried out by the Economic Commission for Latin America and the Caribbean (ECLAC). The results reflect that a company or organization that has an ISO 27001 Information Security certification is not necessarily guaranteed the continuity of its business.

Keywords: Information security, business continuity, cybersecurity, globalization.

I. INTRODUCCIÓN

La información almacenada en el ciberespacio es vulnerable a los incidentes en ciberseguridad, los que se han manifestado y afectado a diversas organizaciones y empresas, impactando negativamente en su economía. Un incidente en ciberseguridad "es un evento o serie de eventos inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio, provocando una pérdida o uso indebido de información, así como interrupción parcial o total de los sistemas" (Universidad Veracruzana, 2023).Un evento de tal magnitud origina pérdidas de los activos digitales de una organización ,hecho que implica que enfrente elevados costos para su recuperación, y más aún, la expone peligrosamente a pérdida de información sensible.

En los últimos años se ha visto un aumento de incidentes informáticos que tienen relación con la seguridad y vulnerabilidad de la información. Como consecuencia de esta nueva realidad, las empresas están desarrollando esfuerzos para mantener la continuidad del negocio y así evitar perjuicios que pueden repercutir en la marca y reputación.

Rodríguez Rojas (2021) sostuvo que: "las empresas están expuestas a diferentes situaciones como fallas, desastres naturales, ataques, crisis económicas, entre otras, por lo que resulta necesario contar con un enfoque proactivo para proteger el negocio de dichos efectos" (p.1).

Según Diaz (2021), "desde el inicio de la pandemia, además de los problemas operativos de los centros logísticos, los ciberataques han aumentado y las actividades logísticas siguen estando entre los sectores económicos más afectados" (p.5).

La Organización de los Estados Americanos (OEA) ha demostrado su interés en temas de ciberseguridad, apoyando investigaciones y fomentando en los países la consigna de proteger la seguridad de su información. El resultado de esta iniciativa fue la elaboración de su guía práctica para Equipos de Respuesta a Incidentes Cibernéticos (Computer Security Incident Response Team (CSIRT), como una manera de contrarrestar eficientemente los ciberataques.

Para tener una mayor aproximación a la situación actual de la seguridad en la red, la presente investigación tiene como objetivo principal realizar un análisis de la seguridad de la información en la gestión de continuidad del negocio con la proyección de implementar un Sistema Integrado de Gestión Multiestándar, que relacione la ISO 27001, enfocada en la seguridad de la información, y la ISO 22301, basada en la continuidad del negocio.

1. Seguridad de la información y ciberataques

De acuerdo a Choi et al. (2018), la implementación de las medidas de seguridad de la información no solamente debe enfocarse en los detalles técnicos, sino también en la visión holística de la organización. Como respuesta a la vulnerabilidad informática, muchos países están desplegando políticas preventivas y celebrando acuerdo con el mismo fin. Según los autores Barrios y Vargas (2018), la Convención o Convenio de Budapest, fue creada en Europa con el respaldo de 60 estados (parte de la Unión Europea, Estados Unidos, Japón Canadá y Australia) para el establecimiento de políticas de prevención del cibercrimen, y de esta manera crear la necesidad de investigar sobre estos delitos, así como promover la cooperación y asistencia internacional cuando estos se presenten. Esta iniciativa llevada a cabo en Hungría y aprobada por el Comité de Ministros del Consejo de Europa, además de buscar la cooperación entre los Estados y el sector privado para protegerse contra el ciberdelito, también contempló la necesidad de proteger legalmente el uso de las tecnologías de la información.

En el Perú existe la Ley de Delitos Informáticos 30096, basada en la tipificación de diversos delitos que a nivel mundial fueron tratados en el Convenio de Budapest (2004) sobre ciberdelincuencia. "Uno de los principales objetivos del Convenio de Budapest es mejorar las condiciones de los países miembros para actuar coordinadamente en el combate contra la cibercriminalidad" (Becker & Violler, 2020, p.79).

Así como el Convenio Internacional de Budapest es la fuente principal que abarca incidentes de delito cibernético, también se tienen normativas para América Latina por parte de la Organización de Estados Americanos (OEA), organismo que a través de su Comité Interamericano contra el Terrorismo (CICTE) y el Programa de Seguridad Cibernética, pretenden el fortalecimiento de las capacidades para la seguridad de la información en sus distintos estados miembros.

La afectación cuando se vulneran los sistemas de seguridad de la información trasciende en todas las organizaciones y empresas, de todos los rubros de la economía. En el caso de las empresas orientadas al sector financiero, surgió la llamada Ley Fintech, impulsada por México y Brasil. Las "Fintech"

se definen como empresas que utilizan tecnología para mejorar los procesos financieros. Según sostuvo Hopkins (2023), es de necesitad prioritaria que se regulen los estándares de ciberseguridad de las entidades financieras a fin de evitar vulnerabilidades en su seguridad de la información, medida preventiva que se deriva de la ley en mención.

Por otro lado, cada país también ha elaborado una legislación de ciber vigilancia, en algunos casos orientados a la protección de datos personales, en especial en el sector salud, en todo lo relacionado a historias clínicas y afines.

Además, es preciso comentar que algunos países cuentan con leyes propias de protección de datos personales, es decir, brindan "protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas" (Instituto Nacional de Desarrollo Social, 2016).

Cabe mencionar que siempre podrán identificarse vulnerabilidades que pueden deteriorar la disponibilidad, integridad y confidencialidad de la información, pero el contar con los procedimientos adecuados y con un plan para la continuidad del negocio, se podría garantizar que la organización supere cualquier eventualidad producto del ciberdelito.

Cuando nos referimos a la continuidad del negocio, estamos considerando el nivel de preparación o reacción inmediata que tiene una empresa u organización para reestablecer o mantener sus funciones principales, luego de algún incidente, desastre o emergencia

2. Gestión de continuidad del negocio

Cano et al. (2021) manifestaron que:" La gestión de la continuidad del negocio es un proceso que identifica las potenciales amenazas a una organización y el impacto que estas podrían causar en las operaciones del negocio si llegan a materializarse" (p.4).

También como una estrategia a nivel organizacional que logra en las empresas el poder afrontar crisis y recomponerse en el menor tiempo posible y sin afectar su calidad de servicio.

Estas crisis o eventos adversos pueden ser producidos por desastres naturales, cortes de energía, virus informáticos, caída del internet o del servidor.

Tomando como referencia los resultados de la CEPAL con respecto a incidentes de ciberseguridad ocurridos en las cadenas logísticas en América Latina, tenemos los siguientes resultados por país afectado:

Tabla 1

Cantidad de incidente por país afectado

País afectado	Número de incidentes
Brasil	11
Chile	11
Argentina	9
México	8
Perú	7
Panamá	5
Uruguay	5
Colombia	4
Ecuador	3
Rep. Dominicana	3

Nota: Adaptado de la CEPAL

Cuando Cepal profundizó su investigación sobre la causa de los incidentes de ciberseguridad, identificó que un 60% corresponden o tiene su origen en la falta de capacitación a los usuarios sobre el uso de la tecnología, es decir, fueron afectados por casos de phishing (31%) y robo de credenciales (29%).Para superar estos incidentes, es recomendable implementar un procedimiento de seguridad de información donde se brinde la orientación necesaria y para poder contrarrestar los ataques de ciberseguridad.

Así también, es importante conocer el tiempo en el cual la empresa u organización demora en volver a la normalidad, a retomar sus actividades con toda confianza y habiendo superado la vulnerabilidad y sus sistemas, reincorporarse en sus gestiones a fin de proporcionar una seguridad de la información.

Tabla 2

Tiempo de recuperación de incidente

En minutos	Algunas horas	Un día	Una semana	Un mes a más tiempo	No lo sabe
4.50%	31.80%	4.50%	9.10%	9.10%	40.90%

Nota. Fuente CEPAL

Cepal desarrolló investigaciones basadas en un concepto llamado "ciber inmunidad", el cual, si lo relacionamos con el Sistema de Gestión de Riesgos, se concluye que el riesgo no se elimina, sólo

se controla y se trata de minimizar el impacto. Para desarrollar estrategias adecuadas para la implementación o medidas de seguridad de la información que esté acorde a las necesidades de la organización, se deben identificar las que correspondan a cada área e integrarlas, siendo el rol del líder determinante en las decisiones que se adopten. De acuerdo a lo indicado por Mahecha-Lagos (2022) , “los líderes de gestión deben desarrollar la capacidad de integrar los sistemas de gestión de una manera eficiente, liviana, ágil que permita generar beneficios y competitividad y no convertirse en una carga para las organizaciones”(p.13).

Por su parte la OEA recomienda “contar con un Equipo de Respuesta a Incidentes Cibernéticos (Computer Security Incident Response Team - CSIRT) puede marcar la diferencia en la respuesta coordinada y eficiente frente a un ataque, y así ayudar a mitigar las consecuencias de este” (2023).

Finalmente, Allianz (2023) informa que los principales riesgos para el año 2023 a nivel mundial son incidentes cibernéticos (34%) e interrupción en el negocio (34%). Cabe mencionar que desde el 2018 se mantiene entre los primeros lugares estos dos tipos de riesgos a nivel mundial.

Con base a lo anteriormente expuesto, se requieren de medidas de seguridad para evitar la vulneración de la información en la red. Jara y Jorquera (2021) sostuvieron que “dada la amplitud de las acciones u omisiones que pueden generar amenazas a la seguridad de los sistemas de información y, eventualmente, concretarse en una fuga de datos, por ejemplo, el riesgo de ocurrencia de estas es constante y requiere de un proceso de gestión continua” (p.206).

La importancia de un plan de continuidad es establecer las estrategias y procedimientos que deben ser implementados por un equipo interdisciplinario que brinde la orientación, apoyo y equipamiento (Rodríguez Rodríguez, 2020).

De acuerdo con Vásquez (2020), en un plan de contingencia informático se proporcionan los procedimientos necesarios para la prevención y reducción de los riesgos

LA OEA menciona que se debe “Orientar los procesos y procedimientos a metodologías ágiles que permitan mejorar los tiempos de respuesta en la atención de incidentes cibernéticos”.

También es preciso mencionar que el inicio de todo este proceso debe ser el identificar nuestra realidad, es por ello que proponemos en el anexo 01 un cuestionario como una evaluación inicial dirigidos a los responsables de TI/Sistemas sobre la seguridad de la información.

Teniendo en consideración que la Organización Internacional de Normalización (ISO) ,creada para la normalización y estandarización de la calidad y seguridad en los bienes y servicios, el objetivo principal de la presente investigación es realizar un análisis de la seguridad de la información en la gestión de continuidad del negocio con la proyección de implementar un Sistema Integrado de Gestión Multiestándar, que relacione la ISO 27001 enfocada en la seguridad de la información y la ISO 22301 basada en la continuidad del negocio.

II. MÉTODOS

El método de la presente investigación es exploratorio y su diseño es no experimental porque no se va a alterar, inducir o modificar las variables.

La recolección de información se realizó con base a datos obtenidos de diversas investigaciones a nivel de América Latina y el Caribe, así analizaremos datos proporcionados por la OEA y la CEPAL.

El desarrollo de la investigación está basado en el análisis de la norma ISO/IEC 27002:2022 seguridad de la información, ciberseguridad y protección de la privacidad. Esta norma se relaciona con la seguridad de la información que proporciona un conjunto de referencia de controles genéricos de seguridad, incluida una guía de implementación (ISOTools 2023). Esta norma es certificable a través de la ISO 27001.

La norma ISO 27002:2022 se centra en las buenas prácticas para la gestión de la seguridad de la información,

Esta norma es una guía tipo check list que está conformado por controles y atiende a los 14 dominios, 35 objetivos de control y 114 controles.

Dentro de la norma ISO 27002, tomaremos para nuestra investigación los aspectos de seguridad de la información en la gestión de continuidad del negocio**,** los ubicaremos dentro de los controles de la Norma ISO 27002 con el número de dominio 17, a los que le corresponden 3 controles.

Tabla 3

Controles Continuidad de la Seguridad de la información.

17.1 Continuidad de la seguridad de la información. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la Información.

Nota. Norma ISO 27002:2022

III. RESULTADOS

Continuidad de la Seguridad de la información

Ante todo, debe tenerse en cuenta que tanto las normas de continuidad del negocio ISO 22301 como la de seguridad de la información ISO 27001 deben estar integradas, de esta manera, al complementarse, el mayor beneficiado será la empresa u organización.

Requisito 17.1.1. Planificación de la continuidad de la seguridad de la información

La planificación comprende las acciones que deben realizarse para proteger y garantizar los datos y sistemas de Planificación de Recursos Empresariales (cuyas siglas en inglés es ERP) que tienen las empresas u organizaciones y que, al momento de ocurrir una incidencia, ataque cibernético, desastre natural o fenómeno meteorológico, puedan continuar sus operaciones de manera normal con la finalidad de no alterar la atención al cliente final.

La continuidad del negocio es un riesgo muy importante que preocupa al 47,2% de las empresas latinoamericanas. En gran medida esos riesgos vienen derivados de problemas con la ciberseguridad. (ISOTools,2023)

Teniendo como antecedente la investigación de Cepal (2023), donde se identificó que un 60% de los incidentes corresponden o tiene su origen en la falta de capacitación a los usuarios sobre el uso de la tecnología

Del mismo modo, con respecto a la continuidad del negocio, el estudio de CEPAL indicaba que un 32% de los afectados, se demoraban solo horas en reestablecer la operatividad ante algún incidente de ciberseguridad. Es por ello, que proponemos en el anexo 02 un cuestionario como una evaluación inicial dirigidos a los responsables de tecnologías de la información (TIs).

Requisito 17.1.2. Implementación de la continuidad de la seguridad de la información

Si nuestra empresa u organización cuenta con una Planificación de Recursos Empresariales (ERP en inglés), ya se dio un gran paso, porque por lo general las bases de datos se encuentran en la nube, es decir, no les afectaría un desastre natural.

Otro factor importante es la trazabilidad de las operaciones ingresadas por el usuario, así ante una interrupción, podrá determinarse en qué proceso se detuvo.

Por otro lado, mientras el ERP sea más completo se puede tener respaldo de la información histórica y recuperar rápidamente sus bases de datos. Por ejemplo las nueva versión de SAP llamado HANA permite replicar las bases de datos en otro servidor (físicamente en otro lugar) o en la nube tiene; además los respaldos se van creando periódicamente y así no toda la información estaría perdida en caso un incidente cibernético y el impacto a la continuidad del negocio sería menor (Novis, 2023).

Así mismo, se debe implementar un “plan con medidas concretas para restablecer la disponibilidad de la información en unos plazos identificados mediante unos planes de respuesta ante emergencias que tengan en cuenta la organización y sus recursos” (ISO 27001:2019).

Requisito 17.1.3. Verificar, revisar y evaluar la continuidad de la seguridad de la información

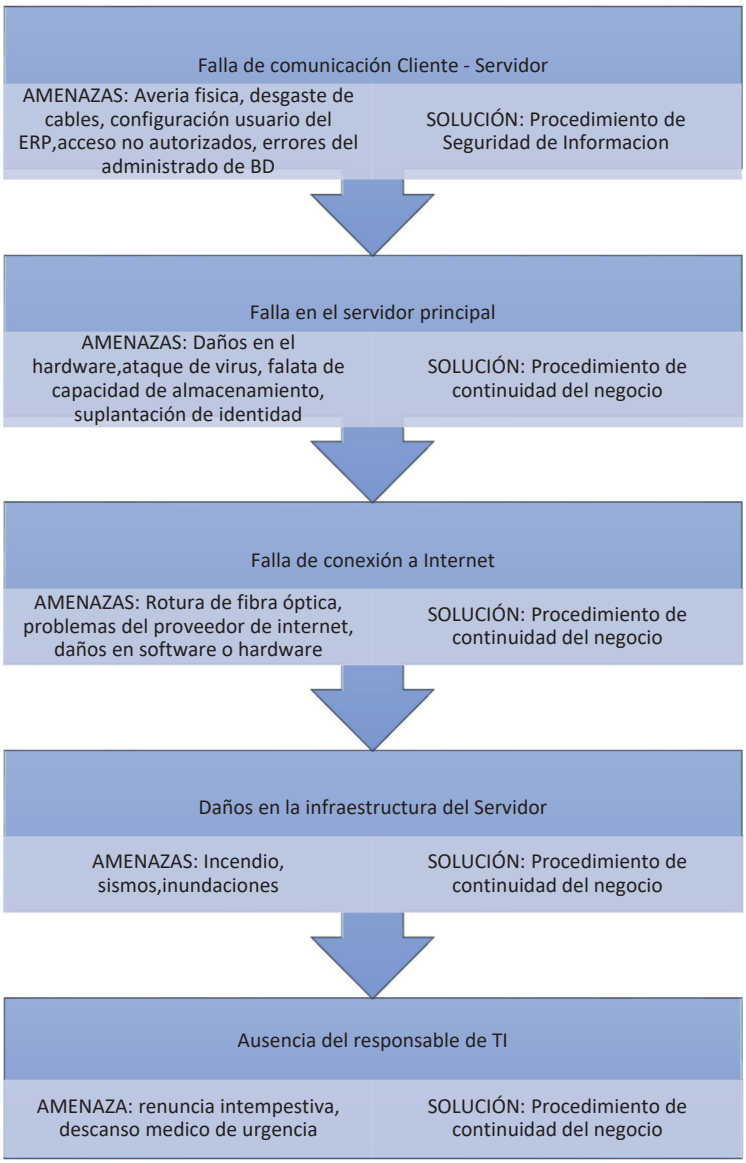
A continuación, se podrá observar las causas y principales amenazas que afectarían la seguridad de la información en la continuidad del negocio y a su vez el procedimiento que debe emplearse respectivamente. Si bien cada causa y amenaza corresponde a un plan distinto; ambos pueden complementarse para un mejor tratamiento dentro de la empresa u organización (ver Figura 1).

IV. DISCUSIÓN

Los resultados del estudio demuestran que si bien a nivel de América Latina las empresas tienen un plan de seguridad de la información o un plan de contingencias y un tiempo estimado de recuperación ante un incidente; no es recomendable limitarse solo a “un conjunto de métodos destinados a proteger la información privada para que no caiga en las manos equivocadas” (Ciberseguridad,2023).

Figura 1

Causas y amenazas a la seguridad de información



Nota. Elaboración propia

Por otro lado, las empresas que van en vanguardia de la seguridad de información, cuentan con un Plan de respuesta a incidentes, cuyo objetivo es dar respuesta a incidentes y evitar ciberataques antes de que se produzcan y minimizando el coste y la disrupción del negocio asociados a los ciberataques que (International Business Machines Corporation, IBM,2023).

Este estudio no está limitado a solo trabajar en ciberseguridad, identificar vulnerabilidades, concientizar al personal que sigue las pautas de seguridad y mantener sus password, entre otros; sino más bien en complementar dos Sistemas integrados de Gestión de Seguridad y Continuidad de Negocio, para que ambos brinden mayor valor agregado a la empresa u organización.

Es decir, siempre garantizando la confidencialidad de la información, la integridad y la disponibilidad del sistema y además con la capacidad de continuar su operatividad en momentos que se ve afectado por un ciberataque, pandemia, desastre natural o interrupción de energía eléctrica o señal de internet.

Es allí donde se ve la mejora continua, donde la seguridad de la información pasa a un nivel superior

garantizando la continuidad del negocio, no solo dando una solución del momento sino marcando pautas para el futuro de la organización en materia de información.

Brindando estrategias y procedimientos que van a permitir incluso que un evento fortuito pase desapercibido. Una integración de los sistemas de seguridad de la información y de continuidad el negocio va permitir desarrollar una política, procedimientos y flujogramas de actividades de respuestas orientadas al acceso continuo sin interrupciones.

V. CONCLUSIONES

Implementar el Sistema de Gestión de Seguridad de la Información no garantiza los objetivos de la continuidad del negocio.

La globalización permite enfocar problemas comunes que afectan a distintas empresas sin límites fronterizos, pero las soluciones deben ser también globales, como la adopción de estándares de sistemas de gestión que brindan las normas ISO.

Los requisitos de la norma 27001 Seguridad de la Información y 33201 Continuidad de Negocio, son aplicables para cualquier país de América Latina, por ende, las normas complementarias (por ejemplo, ISO 27002) no certificables, sirven de guía como parte de la mejora continua.

La planificación para la continuidad del negocio debe formar parte de la principal estrategia de las organizaciones para tener la capacidad de protegerse ante eventuales ciberdelitos, o, en su defecto, aminorar los impactos negativos que se podrían originar por un ataque inevitable.

AGRADECIMIENTOS

El presente trabajo fue financiado por recursos propios de los autores, declarando de haber recibido migan tipo de ayuda económica de alguna persona o institución en particular.

Un agradecimiento especial a las hijas de los autores cónyuges Sr Manuel Pumasunco y Sra. Candy Seminario; y así mismo al núcleo familiar del Sr. Renato Guerra.

REFERENCIAS

[1] Barrios Achavar, V., & Vargas Cárdenas, A. (2018). Convenio sobre la Ciberdelincuencia: Convenio de Budapest. *Asesoría Técnica Parlamentaria*,1-12.

[2] Becker Castellaro, S., & Violler Bonvin, P. (2020) La implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19. 223.Revista *de Derecho Universidad de Concepción,248*,75-112. DOI: 10.29393/RD248-13ICSB20013

[3] Cano Sotomayor, E. et al. (2021). Gestión de la continuidad de negocio: caso Ravmar Freight del sector logístico. *Revista de Ciencias de la Gestión 16*:1-15. https://doi.org/10.18800/360gestion.202106.014

[4] Choi, S.E., Martins, J.T. & Bernik, I. (2018). Information security: Listening to the perspective of organizational insiders. J*ournal of Information Science, 44*(6),752-767. https://doi.org/10.1177/0165551517748288

[5] Díaz, R. (2021). *Estado de la ciberseguridad en la logística de América Latina y el Caribe*. CEPAL. https://repositorio.cepal.org./server/api/core/bitstreams/4b04fcfe-c0f3-4c97-af14-2c234857f433/content

[6] Guía práctica para CSIRTs, (2023). Un modelo de negocio sustentable. https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20ESP%20Digital.pdf

[7] Hopkins, J.J. (15 de mayo de 2023). ¿Por qué es necesaria una Ley Fintech para el Perú? *El Comercio*. https://elcomercio.pe/economía/opinión/por-que-es-necesaria-una-ley-fintech-para-el-peru-por-juan-jose-hopkins-opinion-noticia/

[8] International Business Machines Corporation, 2023 ¿Qué es la respuesta a incidentes? https://www.ibm.com/es-es/topics/incident-response

[9] Instituto Nacional de Desarrollo Social (15 de agosto de 2016). https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

[10] ISOTools Excellence (2023). ISO/IEC 27002:2022 Controles Organizacionales. Todo lo que necesita saber. https://www.isotools.us/2022/07/29/iso-iec-270022022-controles-organizacionales-todo-lo-que-necesitas-saber/

[11] ISOTools Excellence (2023). Riesgos más importantes para las organizaciones en Latinoamérica. *Blog especializado en Seguridad de la Información y Ciberseguridad.* https://www.pmg-ssi.com/2023/04/riesgos-mas-importantes-para-las-organizaciones-en-latinoamerica/

[12] Jara Fuentealva, N. & Jorquera Cruz, A. (2021). La responsabilidad de la Administración del Estado por incidentes de ciberseguridad. *Revista Chilena de Derecho y Economía,10* (1),201-230. DOI 10.5354/0719-2584.2021.58776

[13] Mahecha-Lagos, N.C. (2022). Transformando el futuro: Tendencias emergentes en los sistemas de gestión y el rol clave de sus líderes. *Signos, Investigación en Sistemas de Gestión, 15*(2),11-14. https://doi.org/10.15332/24631140.8862

[14] Novis (2023) Gestión empresarial. https://www.novis.com.mx/blog/gestion-empresarial/plan-de-continuidad-de-negocio-como-te-ayuda-sap-12002/

[15] Organización de Estados Americanos, Programa de Ciberseguridad, 2023.Disponible en https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

[16] Rodríguez Rojas, Y. (2021). Continuidad del negocio: conceptualización y metodologías de evaluación. *SIGNOS-Investigación en Sistemas de Gestión, 13*(1), 1-20. https://doi.org/10.15332/24631140.6337

[17] Rodríguez Rodríguez, C. (2020). La importancia de un plan de continuidad del negocio. *Universidad Piloto de Colombia*,1-10. http://repositorio.unipiloto.edu.co/handle/20.500.12277/9547

[18] Universidad Veracruzana (26 junio, 2023) Coordinación de Gestión de Incidentes de Ciberseguridad. https://www.uv.mx/csirt/que-es-un-incidente-de-ciberseguridad/

[19] Vásquez, A. (2020). *Diseño e implementación de un plan de contingencia informático para mejorar la disponibilidad de los sistemas críticos de la OGTI-MTC* [Tesis de Maestría, Universidad Peruana de Ciencias e Informática]. http://repositorio.upci.edu.pe/handle/upci/127

[20] VMware (2023) Glosario de términos. https://www.vmware.com/es/topics/glossary/content/business-continuity.html

Conflicto de interes de los autores

No existe ningún conflicto de interés por parte de los autores con respecto a la investigación realizada, ni prejuicio o tendencia alguna sobre los resultados obtenidos.

Contribución de los autores

En el aporte de los autores destaca la amplia experiencia en las normativas ISO de la Sra. Candy Seminario, así mismo la profundidad en la investigación del Mg. Manuel Pumasunco con amplia experiencia en implementación de ERPs y Sistemas de Información Gerencial.

Finalmente, la parte metodológica y diseño de la investigación estuvo a cargo del Sr. Renato Guerra.

La participación del equipo de autores permitió la redacción y revisión final de la investigación.