ARTÍCULO ORIGINAL

ANÁLISIS DE INFORMACIÓN DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD EN ORGANIZACIONES

ANALYSIS OF THE INFORMATION BY THE MANAGEMENT OF SECURITY INCIDENTS IN ORGANIZATIONS

ANALYSIS OF SECURITY INCIDENT MANAGEMENT INFORMATION IN ORGANIZATIONS

Tasa Catanzaro, María Elena; Maquera Quispe, Henry George; Rojas Bujaico, John Fredy; Delgado Rospigliosi, Marjorie Gabriela del Carmen

María Elena Tasa Catanzaro
c20968@utp.edu.pe
Universidad Tecnológica del Perú, Perú

Henry George Maquera Quispe
hmaquera@uncp.edu.pe
Universidad Nacional del Centro del Perú, Perú

John Fredy Rojas Bujaico
john.rojas@unh.edu.pe
Universidad Nacional de Huancavelica, Perú

Marjorie Gabriela del Carmen Delgado Rospigliosi
delgado.mg@pucp.edu.pe
Pontificia Universidad Católica del Perú, Perú

Puriq
Universidad Nacional Autónoma de Huanta, Perú
ISSN: 2664-4029
ISSN-e: 2707-3602
Periodicidad: Cuatrimestral
vol. 4, e196, 2022
revistapuriq@unah.edu.pe

Recepción: 17 Mayo 2021
Aprobación: 20 Agosto 2021
Publicación: 04 Enero 2022

URL: http://portal.amelica.org/ameli/journal/514/5142970003/

DOI: https://doi.org/10.37073/puriq.4.1.196

Autor de correspondencia: c20968@utp.edu.pe

Resumen: Los incidentes de seguridad en una organización se consideran como la fuente principal para evaluar la correcta aplicación de los controles de seguridad en organizaciones públicas o privadas. La investigación está basada en el comportamiento de los incidentes ante la participación de controles de tecnologías de información conjuntamente con los procesos formales en las organizaciones. Se utilizaron buenas prácticas de seguridad basadas en las normas internacionales ISO/IEC 27001 e ISO/IEC 27002. Se aplicó la metodología Magerit v3 y técnicas de inteligencia de negocios para integrar y procesar la información obtenida a través de fuentes heterogéneas de información implementadas en las organizaciones bajo estudio. La información obtenida se estableció en 9 controles de seguridad comunes a las organizaciones en estudio aplicados bajo un estudio experimental. El análisis de los datos permitió establecer que el constante monitoreo y supervisión de la aplicación de los controles de seguridad eleva los niveles de seguridad en las organizaciones garantizando la continuidad de los servicios y procesos.

Palabras clave: buena práctica, incidente, información, seguridad.

Abstract: Security incidents in an organization are considered the main source for evaluating the correct application of security controls in public or private organizations. The investigation is based on the behavior of the incidents before the participation of information technology controls together with the formal processes in the organizations. Good security practices based on the international standards ISO / IEC 27001 and ISO / IEC 27002 were used. The Magerit v3 methodology and business intelligence techniques were applied to integrate and process the information obtained through heterogeneous sources of information implemented in the organizations under study. The information obtained was established in 9 security controls

CITAR COMO: Tasa Catanzaro, M. E., Maquera Quispe, H. G., Rojas Bujaico, J. F., & Delgado Rospigliosi, M. G. del C. (2022). Análisis de información de la gestión de incidentes de seguridad en organizaciones . *Puriq, 4*, e196. https://doi.org/10.37073/puriq.4.1.196

common to the organizations under study applied under an experimental study. The analysis of the arrival data will establish that the constant monitoring and supervision of the application of the security controls raises the security levels in the organizations that guarantee the continuity of the services and processes.

Keywords: good practice, incident, information, security.

Resumo: Os incidentes de segurança em uma organização são considerados como a principal fonte para avaliar a aplicação correta dos controles de segurança em organizações públicas ou privadas. A pesquisa baseia-se no comportamento de incidentes envolvendo controles de TI em conjunto com processos formais nas organizações. Foram utilizadas boas práticas de segurança baseadas nas normas internacionais ISO/IEC 27001 e ISO/IEC 27002. A metodologia Magerit v3 e as técnicas de business intelligence foram aplicadas para integrar e processar as informações obtidas de fontes heterogêneas de informações implementadas nas organizações em estudo. As informações obtidas foram estabelecidas em 9 controles de segurança comuns às organizações em estudo, aplicados em um estudo experimental. A análise dos dados permitiu estabelecer que o monitoramento e a supervisão constantes da aplicação dos controles de segurança elevam os níveis de segurança nas organizações, garantindo a continuidade dos serviços e processos.

Palavras-chave: good Practice, incident, information, security.

INTRODUCCIÓN

La información se ha transformado en un activo muy importante dentro de una organización debido a que es un insumo vital para que los servicios de tecnologías de información (TI) puedan operar de manera necesaria (Ali et al., 2019). La información ha venido siendo categorizada bajo los niveles de *ultrasecreta*, secreta, confidencial y no clasificada debido a su participación en diferentes tipos de servicios de TI tomando como referencia la metodología Magerit v3.

La participación de la información se ha hecho evidente en diversos procesos y servicios de una organización, por lo cual esta debe ser protegida mientras se encuentre en reposo o en movimiento. Por ello, diversas organizaciones han incorporado profesionales especializados que analizan los niveles de riesgos e impacto ante la presencia de amenazas que exploten vulnerabilidades existentes (da Veiga et al., 2020). De igual manera, diversos ejecutivos y responsables de los activos de TI están gestionando la información generada por los controles de seguridad, lo cual les ha permitido mejorar su capacidad en la toma de decisiones (Caseiro y Coelho, 2019).

Las organizaciones se encuentran implementando sistemas de gestión de seguridad informática (SGSI) que permitan poner en producción controles de seguridad capaces de garantizar los niveles de *confidencialidad, integridad y disponibilidad* de los activos de TI (Ali et al., 2019). Los SGSI implementados se basaron en la norma internacional ISO/EIC 27001, mientras que los controles de seguridad se basaron en la norma ISO/EIC 27002. Sin embargo, la abundancia de datos ha requerido la formulación de mecanismos para categorizar

Notas de autor

Email: c20968@utp.edu.pe

y organizar la información con el fin de evaluar el cumplimiento de los mecanismos de control y garantizar los servicios en la organización (Cheng et al., 2020).

Las organizaciones en la ciudad de Huancayo vienen implementando controles técnicos con el fin de reducir los niveles de riesgo ante ataques a los activos de TI. Sin embargo, los controles técnicos deben ser integrados con controles administrativos y físicos. No obstante, los controles carecen de una buena estrategia de implementación basada en técnicas y marcos de trabajo internacional que garanticen la continuidad del negocio en la organización (Szczepaniuk et al., 2020). De igual manera, la información generada por los controles de seguridad se ha incrementado significativamente y ha traído como consecuencia que se incorporen el uso de herramientas de inteligencia organizacional (Larson y Chang, 2016). La investigación analizó el comportamiento del cumplimiento de controles administrativos, técnicos y físicos que permitieron garantizar la correcta ejecución de los procesos establecidos por la organización (Cobb et al., 2018). Los controles bajo estudio estuvieron basados en la norma internacional ISO/EIC 27002:

- *Políticas*. Documento aprobado por la organización que expresa una intención e instrucción global.
- *Organización*. Establece la administración de la seguridad de la información con el fin de alinear los objetivos y actividades de la organización.
- *Recursos Humanos.* Fomenta la educación e informar al personal desde su incorporación.
- *Activos.* Fomenta que la organización obtenga conocimiento detallado sobre los activos necesarios para impulsar sus procesos.
- *Accesos*. Controla el acceso a través de controles basados en restricciones y excepciones.
- *Cifrado.* Fomenta el uso de técnicas criptográficas para proteger la información sobre un análisis de riesgos.
- *Física y ambiental.* Minimiza riesgos de datos e interferencias de información durante las operaciones en una organización.
- *Operativas.* Brinda control de la ejecución de procedimientos de operaciones, desarrollo y mantenimiento de la documentación relacionada.
- *Telecomunicaciones.* Asegura la protección de información transmitida a través de la infraestructura tecnológica.
- *Adquisiciones, desarrollo y mantenimiento.* Fomenta la inclusión de controles de seguridad y validación de datos en el desarrollo o adquisición de sistemas de información.
- *Suministradores.* Mantiene los niveles mínimos de los servicios contratados y entregados por terceros.
- *Incidentes.* Garantiza la comunicación de eventos se seguridad y debilidades asociados a sistemas de información.
- *Continuidad de negocios.* Preserva la seguridad de TI dentro de las etapas de activación, desarrollo de procesos, procedimientos y planes de continuidad.
- *Cumplimiento.* Fomenta la incorporación de disposiciones legales y contractuales en el diseño, operaciones, uso y administración de sistemas de información.

MÉTODOS

El método utilizado en esta investigación fue el *analítico* debido a que la estrategia adoptada consistió en descomponer los dominios establecidos por las normas ISO/IEC 27001 e ISO/IEC 27002. De igual manera se ha utilizado el método inductivo como método científico debido a que se han logrado conclusiones generales a partir de premisas particulares de los escenarios de estudio.

La investigación se inició mediante la aplicación de los diferentes niveles de negocio de la organización en relación a una arquitectura de TI que fue representada a través de la figura 1. Una arquitectura de TI opera de manera sincronizada entre áreas de gestión y gobierno aislada con el fin de lograr el cumplimiento de las metas de la organización (Ramalingam et al., 2018). La arquitectura de TI se ha convertido en un nexo entre los

niveles tácticos y operativos de la organización puesto que permite un alineamiento detallado de los activos, procesos y servicios de TI (Polyvyanyy et al., 2017).

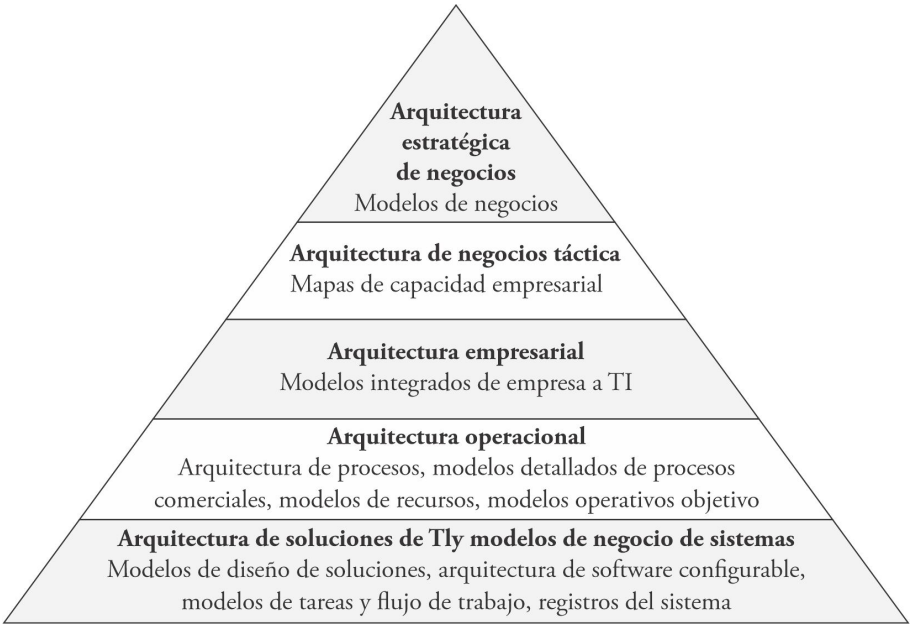

FIGURA 1

Procesos en diferentes niveles de la pirámide organizacional

Nota. El gráfico presenta una estructura aplicable en la gestión de procesos que inicia en una estrategia empresarial hasta llegar a las arquitecturas de TI. Tomado de *Process querying: Enabling business intelligence through query-based process analytics. Decision Support Systems* (p-5), por A. Polyvyanyy.

Para el desarrollo de la investigación se han considerado las etapas presentadas en la figura 2. La retroalimentación participa en cada etapa del modelo propuesto ya que su interacción fomenta la aplicación de experiencias con el fin de implementar un sistema de gestión de seguridad de la información más adecuado. Esta visión sistémica permite establecer medidas que garanticen confidencialidad, integridad y disponibilidad de la información (Dumont et al., 2018).

- Planificación. Esta etapa permite establecer las bases para el desarrollar un plan de seguridad y modelo de sistema de gestión de seguridad.
- Diseño. Establece un plan de seguridad y modelo para un sistema de gestión de seguridad de información y tecnologías de información.
- Operación. Implementa el programa de actividades definido en la etapa de Diseño.
- Retroalimentación. Permite la evaluación de los resultados obtenidos en la culminación de la implementación del plan de seguridad y establecer recomendaciones para mejora.

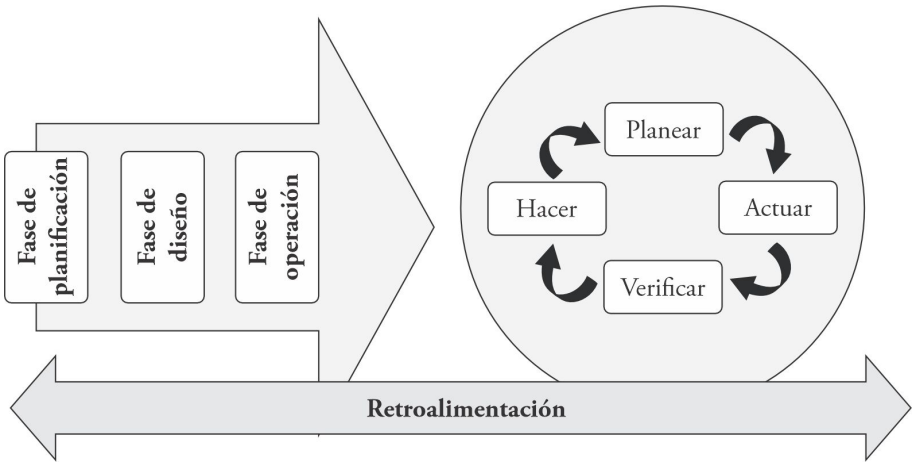

FIGURA 2

Estrategia para la implementación de un SGSI

Nota. El gráfico muestra la interacción entre las diversas etapas en los procesos de implementación de un sistema de seguridad de sistemas de información. Basado en *Sécurité de l'information: autodiagnostic selon l'ISO/ CEI 27001* (p-3) por F. Dumont et al, https://doi.org/10.1016/j.irbmnw.2018.08.001

En el proceso de evaluación de activos de TI relacionados se utilizaron los criterios de valoración propuestos por la metodología Magerit v3.0 que establece una escala de 0 a 10, este valor se basa en relación al efecto de riesgos identificado (Evans et al., 2019). Asimismo, se hizo uso de criterios de evaluación de seguridad de la información basados en:

- Contraseñas
- Protección del puesto de trabajo
- Uso de correo electrónico
- Uso de dispositivos no corporativos
- Uso de redes inalámbricas
- Almacenamiento en los equipos de trabajo
- Aplicaciones permitidas
- Clasificación de la información
- Plan de continuidad de negocios

Para el desarrollo de la investigación se procedió a la recolección de información a través de hojas de cotejo y resúmenes de los reportes de herramientas de software de nivel de monitoreo. Las fuentes de información analizadas fueron de diversos tipos, por lo que se utilizó procesos ETL (Extraer, Transformar y Cargar) para trasladar la información a una estructura de almacenamiento que permita iniciar con el tratamiento de la información (Lukić et al., 2016).

Se utilizó un modelo basado en inteligencia de negocios para iniciar el tratamiento de información que está representada en la figura 3. Esta estrategia para el tratamiento de datos se fundamentó en la combinación de la arquitectura de las bases de datos, análisis de negocios y visualización de datos que permiten extraer conocimiento de los datos existentes (Vajirakachorn y Chongwatpol, 2017). El marco de trabajo propuesto permite estandarizar y procesar datos con el fin de formular decisiones estratégicas (Lopes et al., 2020). El marco de trabajo se basó en las siguientes etapas:

- Paso 1. Establecer los objetivos de la organización.
- Paso 2. Establecer las métricas de rendimiento vinculadas a los controles de seguridad en las organizaciones.
- Paso 3. Recopilación de información relevante para el análisis de los incidentes de seguridad.
- Paso 4. Integración de información de diversas fuentes.
- Paso 5. Presentación de información de manera clara y concisa.

- Paso 6. Identificación de patrones de comportamiento de la información procesada.

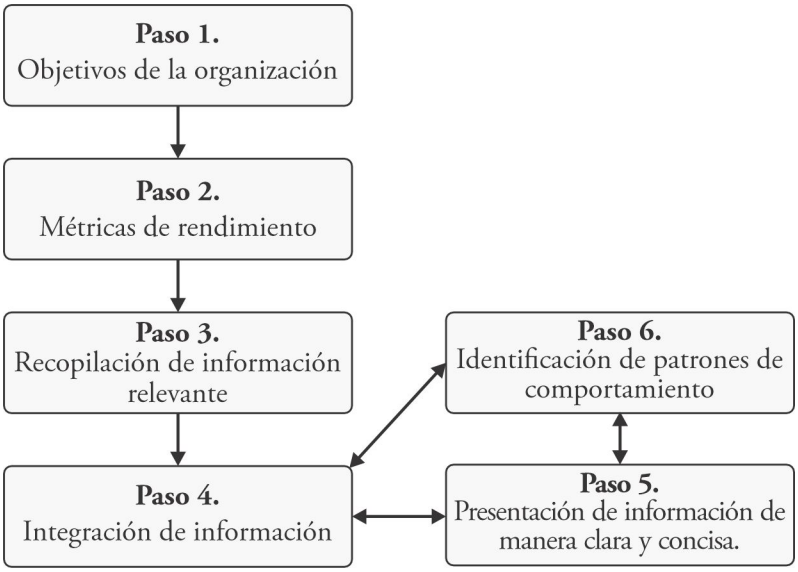

FIGURA 3

Marco de trabajo de Inteligencia de negocios

Nota. El gráfico presenta la secuencia para un marco de trabajo de inteligencia de negocios. Esta secuencia es utilizable para el desarrollo del análisis de la información.

RESULTADOS

Se ha procedido a realizar evaluaciones bajo los criterios de seguridad de la información propuestos. Para esto se han estudiado 02 organizaciones públicas y 02 organizaciones privadas como escenario de acción. Se dispuso el análisis de la información de 09 controles de TI que son comunes a las organizaciones bajo estudio. El análisis de los controles de TI se estableció bajo las categorías que son comunes a las organizaciones con el fin de tener criterios similares para realizar un análisis organizado e integrado. La Tabla 1 presenta los porcentajes de incremento o decremento en la aplicación de los controles de seguridad formalizados.

TABLA 1
Evaluación del uso de control de Tecnologías de Información

Categorías	Organización Pública 01	Organización Pública 02	Organización Privada 01	Organización Privada 02
Contraseñas No utilizar las contraseñas por defecto	22.00%	34.00%	14.00%	21.00%
No compartir las contraseñas con nadie	-46.00%	-64.00%	-16.00%	-16.00%
No utilizar las contraseñas por defecto	-32.00%	-59.00%	-50.00%	-46.00%
Protección del puesto de trabajo Bloqueo programado de sesión	30.00%	24.00%	17.00%	26.00%
Seguridad de impresoras	31.00%	37.00%	31.00%	23.00%
Directivas de confidencialidad	32.00%	43.00%	20.00%	25.00%
Uso de correo electrónico. Ofuscar direcciones de correo electrónico	-46.00%	-71.00%	-24.00%	-17.00%
Uso adecuado del correo electrónico	43.00%	33.00%	18.00%	23.00%
Uso de dispositivos no corporativos: Acceso a aplicaciones no permitidas	-60.00%	-65.00%	-85.00%	-77.00%
Bloqueo programado	-50.00%	-51.00%	-75.00%	-80.00%
Uso de redes inalámbricas: Acceso a la red - VPN	22.00%	43.00%	26.00%	13.00%
Uso de computadores no corporativos	5.00%	7.00%	27.00%	54.00%
Almacenamiento en equipos de trabajo: Almacenamiento clasificado de información	22.00%	43.00%	26.00%	13.00%
Cifrado de información corporativa	5.00%	7.00%	27.00%	54.00%
Información reportada para copia de seguridad	14.00%	17.00%	42.00%	42.00%
Aplicaciones permitidas: Equipos licenciados	0.00%	0.00%	0.00%	0.00%
Actualización continua	20.00%	11.00%	0.00%	0.00%
Clasificación de la información: Inventario de información	18.00%	10.00%	9.00%	15.00%
Tratamiento de seguridad en producción	12.00%	15.00%	26.00%	24.00%
Plan de continuidad de negocios: Análisis de impacto de negocios	10.00%	10.00%	16.00%	40.00%
Estrategias de continuidad	14.00%	10.00%	8.00%	21.00%
Planes de contingencia en producción	14.00%	10.00%	19.00%	35.00%

Nota. La tabla resume la evaluación de 22 controles de seguridad que tuvieron las organizaciones bajo estudio. Se puede apreciar el comportamiento evolutivo de los resultados de la evaluación durante el estudio.

La categoría contraseñas permitió evaluar los niveles de control en la gestión de contraseñas que son consideradas como el primer punto de acceso de un usuario a los diversos sistemas de información en las organizaciones. En la figura 4 se puede apreciar que la métrica No utilizar contraseñas por defecto ha sufrido una mejor y mayor evolución debido a la participación de estrategias técnicas implementadas en los servidores de las organizaciones.

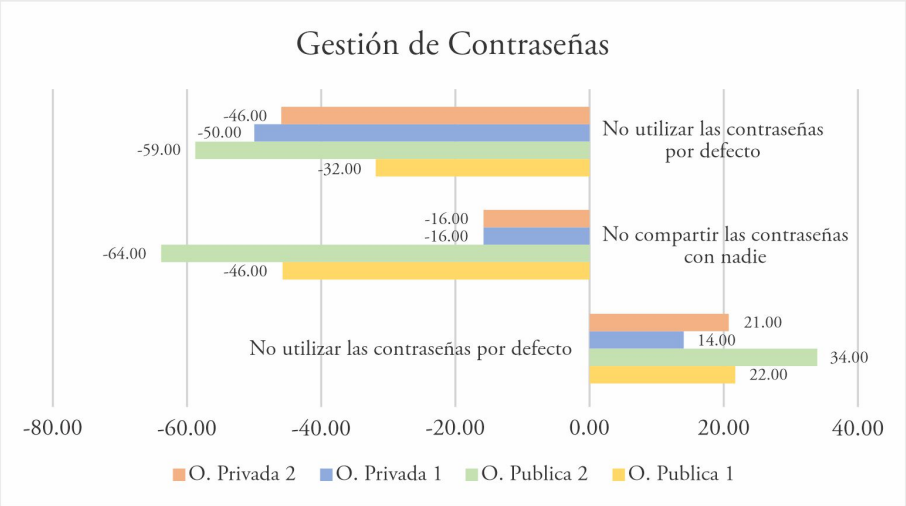

FIGURA 4
Gestión de contraseñas

Nota. El gráfico presenta el cambio de la evaluación de los incidentes relacionados con la categoría Gestión de contraseñas. Los valores negativos indican que se redujeron los incidentes.

La categoría **Protección de puestos de trabajo** permite un monitoreo respecto al control por parte del usuario en las organizaciones. Los mecanismos de control implementados se han basado en la participación responsable de los usuarios por lo que entre organizaciones públicas y privadas se aprecia una mejora homogénea.

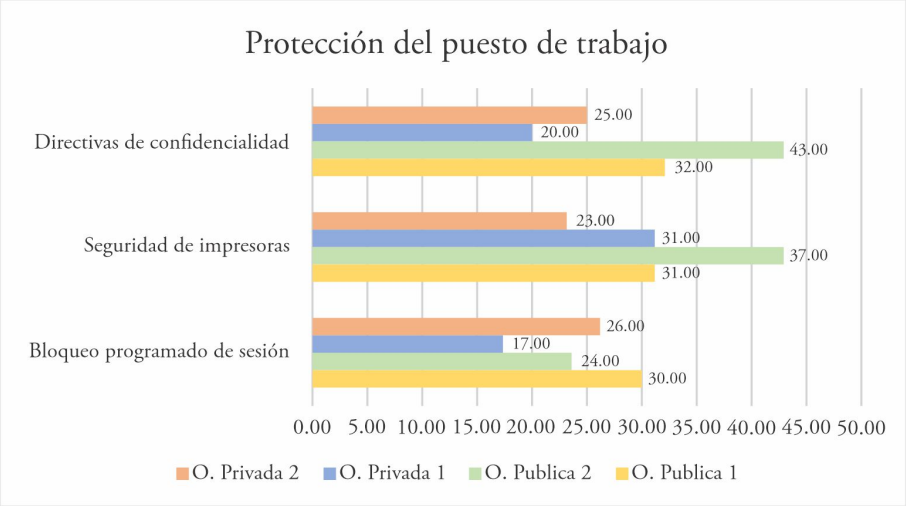

FIGURA 5
Protección del puesto de trabajo

Nota. El gráfico presenta el cambio de la evaluación de los incidentes relacionados con la categoría Protección de puestos de trabajo. Los valores positivos indican que se ha incrementado los niveles de protección.

La categoría **Uso de comercio electrónico** permite evaluar la participación del servicio de correo electrónico para los fines que fue implementado en la organización. La figura 6 sintetiza que este servicio se utilizaba inicialmente de manera muy descuidada; sin embargo, ahora se aprecia una adecuada mejora en el uso de este.

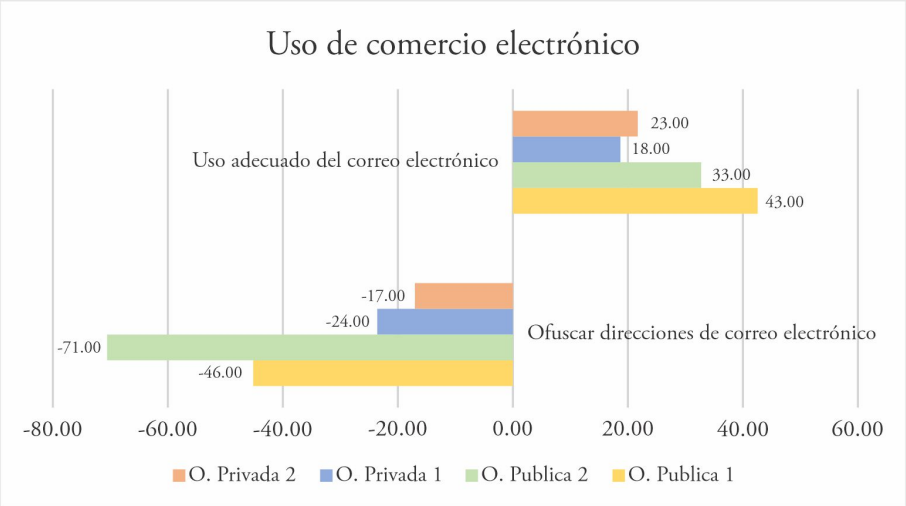

FIGURA 6

Uso de comercio electrónico

Nota. El gráfico presenta el cambio de la evaluación de los incidentes relacionados con la categoría Uso de comercio electrónico. El valor negativo indica que se han reducido la cantidad de incidentes en relación a un determinado control.

La categoría **Uso de dispositivos no corporativos** permite evaluar el uso de dispositivos que no están considerados en el inventario de activos de TI de la organización que tienen acceso a los recursos. La figura 7 resume concretamente la mejora a través de controles técnicos implementados a través de los dispositivos de red en producción dentro de la organización.

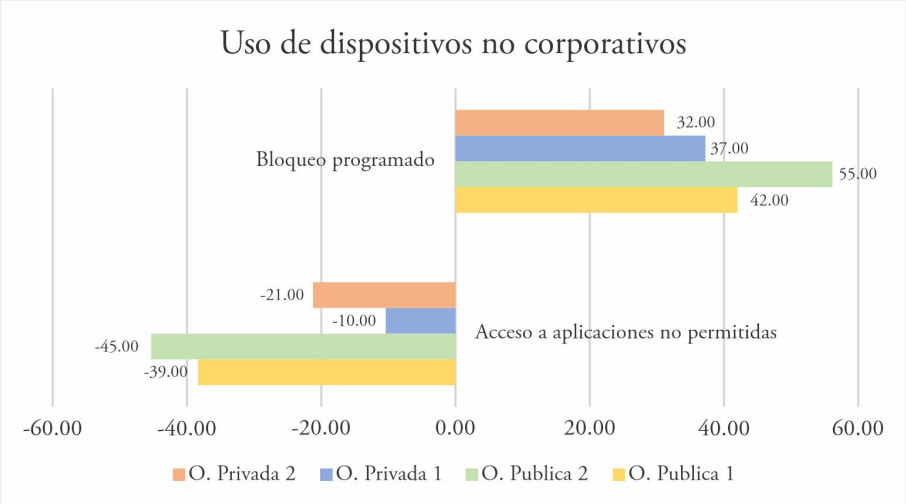

FIGURA 7

Uso de dispositivos no corporativos

Nota. El gráfico presenta el cambio de la evaluación de los incidentes relacionados con la categoría Uso de dispositivos no corporativos. Los valores opuestos indican que los controles han ido mejorando durante el estudio.

La categoría **Uso de redes inalámbricas** permite evaluar el acceso de diversos dispositivos a la red inalámbrica de la organización. La figura 8 permite sintetizar el comportamiento de mejora en el control de

acceso a las redes inalámbricas, por lo que a diversos dispositivos ajenos a las organizaciones no se les permite acceder a los recursos de TI.

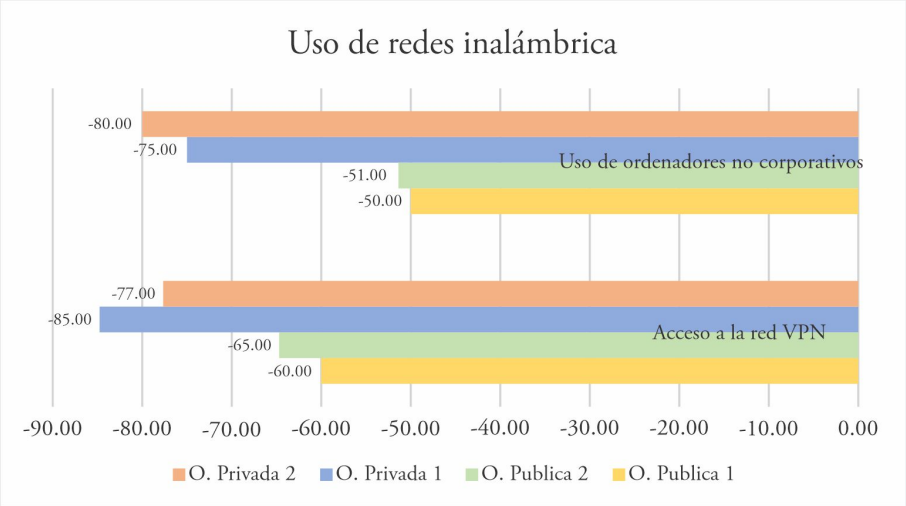

FIGURA 8

Uso de redes inalámbricas

Nota. El gráfico presenta el cambio de la evaluación de los incidentes relacionados con la categoría Uso de redes inalámbricas. Los valores negativos indican que los accesos anónimos a la red inalámbrica se han reducido durante el estudio.

La categoría **Almacenamiento en equipos de trabajo** permite monitorear el uso de los equipos de trabajo en el almacenamiento de información vital para el desarrollo de los procesos en una organización. La Figura 9 muestra el comportamiento de mejora en el control de la información, sin embargo, se aprecia que el uso del cifrado de información en organizaciones públicas es muy reducido.

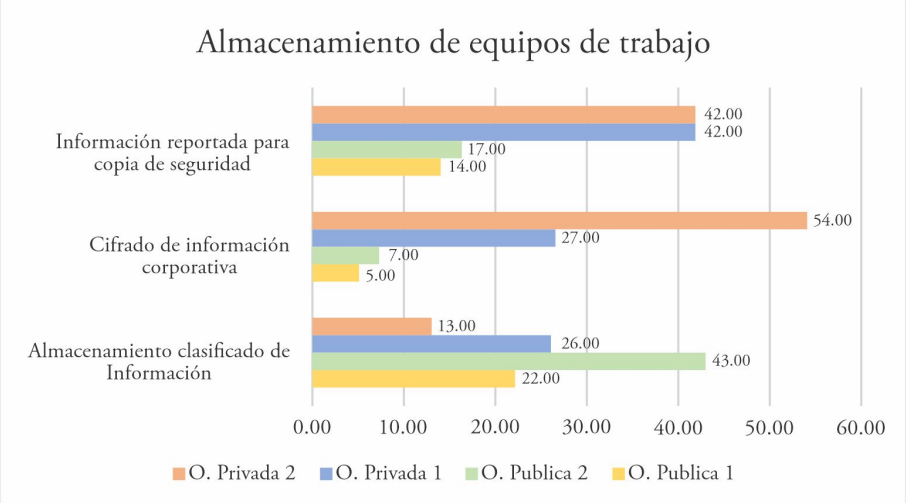

FIGURA 9

Almacenamiento en equipos de trabajo

Nota. El gráfico presenta el cambio de la evaluación de los incidentes relacionados con la categoría Almacenamiento de equipos de trabajo. Los valores positivos indican que se han mejorado los niveles de seguridad de la información existente en las organizaciones.

La categoría **Aplicaciones permitidas** permite estimar el grado de equipos bajo licencia y continuidad de servicios que permitan garantizar los procesos formales en una organización. La figura 10 presenta una que los dos tipos de organización no han evolucionado en los procesos de licenciamiento del software, esto mayormente se debe a la cantidad de inversión necesarias.

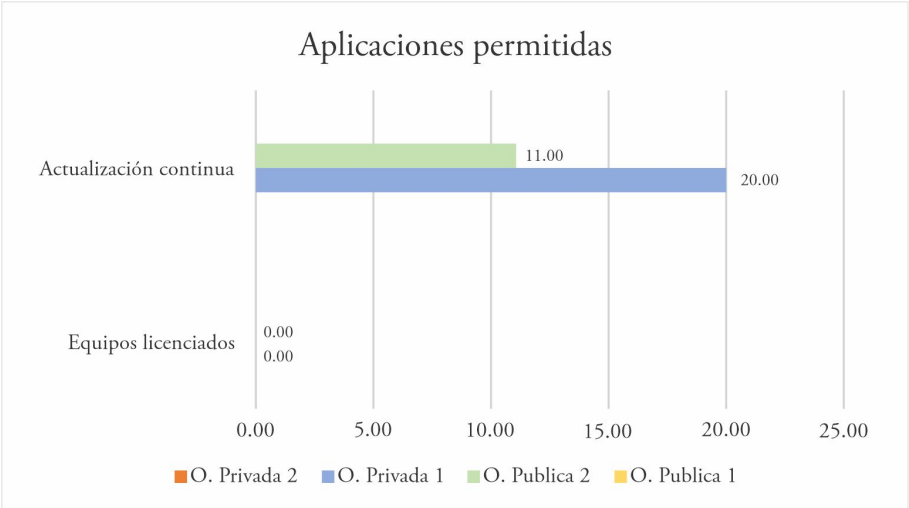

FIGURA 10
Aplicaciones permitidas

Nota. El gráfico presenta el cambio de la evaluación de los incidentes relacionados con la categoría Aplicaciones permitidas. Se aprecia un incremento en la adquisición de las licencias en las organizaciones públicas, mientras que las organizaciones privadas no realizan incrementos.

La categoría **Clasificación de la Información** examina el grado de control de los activos de información en base a una clasificación basada en el valor crítico en la organización. La Figura 11

resume una mejora poco significativa; sin embargo, debe considerarse el grado inicial de clasificación de la información en cada organización.

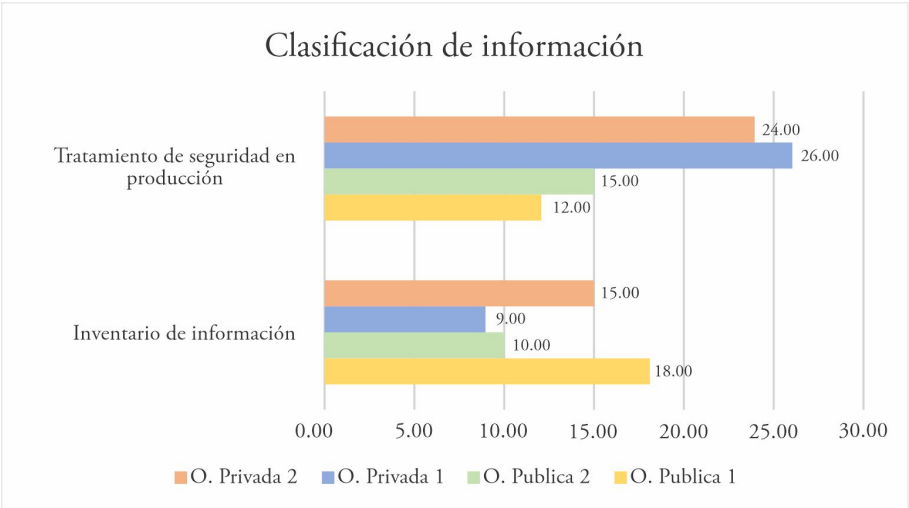

FIGURA 11
Clasificación de la información

Nota. El gráfico presenta el cambio de la evaluación de los incidentes relacionados con la categoría Clasificación de la información. Los valores positivos indican que se ha mejorado los métodos de administración de la información.

La categoría **Plan de continuidad de negocios** valora el grado de garantía en la continuidad de los activos requeridos para que los procesos de las organizaciones puedan ejecutar de manera ininterrumpida en los servicios de TI proporcionados. La figura 12 describe el comportamiento de mejora que ejecutan las organizaciones que garantiza que los procesos de las organizaciones no se detengan.

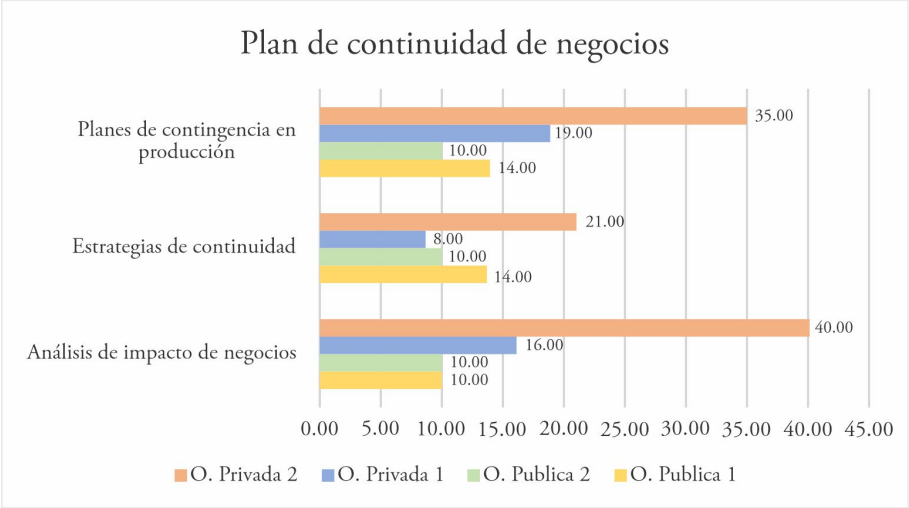

FIGURA 12

Plan de continuidad de negocios

Nota. El gráfico presenta el cambio de la evaluación de los incidentes relacionados con la categoría Plan de continuidad de negocios. Los valores positivos indican que se ha mejorado las estrategias de continuidad.

DISCUSIÓN

La tabla 1 y las figuras 4 al 12 indican que existe una tendencia creciente a mejorar la calidad de los controles de seguridad de TI que permiten que los procesos no se vean afectados ante incidentes cada vez menos presentes. La disminución de incidentes de seguridad ha permitido que los servicios de TI no sean declarados deficientes o que no satisfagan los niveles de gestión de servicios previamente establecidos.

El tratamiento de la información de seguridad es uno de los factores más analíticos debido a su naturaleza confidencial. El uso de mecanismos de control basados en técnicas de cifrado dificulta el acceso a recursos por parte de personal no autorizado de tal forma que se garantice una continua integridad, disponibilidad y confidencialidad (Mall y Saroj, 2018). Este criterio ha sido muy útil para establecer una estrategia de inteligencia de negocios aplicada a los registros de información relacionadas con el desempeño de los mecanismos de control de seguridad, por lo que la aplicación del proceso ETL permitieron lograr un tratamiento de la gran cantidad de información generada con el fin de presentar resúmenes ejecutivos dirigidos a los responsables del área de seguridad de la información.

Un factor muy importante en una organización es el cumplimiento de la confidencialidad, integridad y disponibilidad como objetivo de un programa de seguridad que trae consigo un incremento significativo de los niveles de confianza por parte de los clientes de los servicios proporcionados por las organizaciones (Wu et al., 2013). Esta investigación logra incrementar la confianza de los clientes de las organizaciones a través de la evaluación continua de la aplicación de los controles de seguridad orientadas a proteger y garantizar el continuo servicio proporcionado. La presentación de las evaluaciones periódicas ha permitido a los responsables de los activos y estrategias de seguridad formular mejoras significativas entre los controles de seguridad relacionados con el escenario operativo - organizacional.

El oportuno acceso a información sobre riesgos, ataques, vulnerabilidades, salvaguardas permite mitigar las amenazas. Por lo cual, los responsables del control de riesgos deben procesar una gran variedad de fuentes de datos de información heterogénea. Esta información heterogénea trae como consecuencia una enorme dificultad en los procesos de integración y utilización en los procesos de seguridad y gestión de riesgos (Sauerwein et al., 2019). Por lo que el uso de técnicas de integración de información se hace fundamental para el adecuado procesamiento y el uso apropiado de los controles tecnológicos establecidos. Asimismo,

debe tenerse presente que los servicios de tecnologías de información deben estar formalizados y establecidos como activos dentro de las organizaciones para realizar la continua supervisión y monitoreo correspondiente.

La información que se genera en organizaciones ha impulsado el proceso de transformar datos en conocimiento para mejorar los resultados en las diferentes actividades de una organización (Carvalho et al., 2019). Los datos generados a través de la supervisión y monitoreo de los controles tecnológicos han permitido implementar plataformas de monitoreo que se encargan de registrar incidentes de seguridad que permiten establecer el patrón de comportamiento necesario para garantizar la continua operación de los procesos y servicios de la organización.

CONCLUSIONES

1. El monitoreo y supervisión continua de controles de seguridad fomentan un incremento en la cantidad de información. La cantidad de información debe ser tratada mediante estrategias que permitan la integración e interrelación de fuentes de información heterogéneas, por lo que la aplicación de estrategias de Inteligencia de Negocios es útil para tal fin.

2. El constante monitoreo y supervisión de los controles de seguridad ha permitido concientizar al personal en los hábitos de la seguridad de la información. La implementación de la cultura de la seguridad de la información ha permitido que se incrementen los niveles de seguridad bajo los criterios aplicados en esta investigación. Esto garantiza la continuidad de los servicios formalizados en las organizaciones.

3. La importancia de la presentación de información organizada permite identificar el nivel de cumplimiento de los controles de información entre los servicios de tecnologías de información de las organizaciones. Por lo cual, el uso de técnicas de inteligencia de negocios se ha generalizado y fomentado entre las organizaciones bajo estudio con el fin de lograr un adecuado procesamiento de datos.

REFERENCIA BIBLIOGRÁFICA

Ali, O., Shrestha, A., Chatfield, A., y Murray, P. (2019). Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly. https://doi.org/10.1016/j.giq.2019.101419

Carvalho, J. V., Rocha, Á., Vasconcelos, J., y Abreu, A. (2019). A health data analytics maturity model for hospitals information systems. International Journal of Information Management, 46, 278–285. https://doi.org/10.1016/j.ijinfomgt.2018.07.001

Caseiro, N., y Coelho, A. (2019). The influence of Business Intelligence capacity, network learning and innovativeness on startups performance | Elsevier Enhanced Reader. Journal of Innovation & Knowledge, 4(3), 139–145. https://doi.org/10.1016/j.jik.2018.03.009

Cheng, C., Zhong, H., y Cao, L. (2020). Facilitating speed of internationalization: The roles of business intelligence and organizational agility. Journal of Business Research, 110, 95–103. https://doi.org/10.1016/j.jbusres.2020.01.003

Cobb, C., Sudar, S., Reiter, N., Anderson, R., Roesner, F., y Kohno, T. (2018). Computer security for data collection technologies. Development Engineering, 3, 1–11. https://doi.org/10.1016/j.deveng.2017.12.002

da Veiga, A., Astakhova, L. V., Botha, A., y Herselman, M. (2020). Defining organisational information security culture – Perspectives from academia and industry. Computers & Security, 101713. https://doi.org/10.1016/j.cose.2020.101713

Dumont, F., Jemai, S., Xu, Z., Felan, P. M., y Farges, G. (2018). Sécurité de l'information : autodiagnostic selon l'ISO/CEI 27001. In IRBM News (Vol. 39, Issues 4–5, pp. 90–95). Elsevier Masson SAS. https://doi.org/10.1016/j.irbmnw.2018.08.001

Evans, M., He, Y., Maglaras, L., Yevseyeva, I., y Janicke, H. (2019). Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. International Journal of Medical Informatics, 127, 109–119. https://doi.org/10.1016/j.ijmedinf.2019.04.019

Larson, D., y Chang, V. (2016). A review and future direction of agile, business intelligence, analytics and data science. International Journal of Information Management, 36(5), 700–710. https://doi.org/10.1016/j.ijinfomgt.2016.04.013

Lopes, J., Guimarães, T., y Santos, M. F. (2020). Adaptive business intelligence: A new architectural approach. Procedia Computer Science, 177, 540–545. https://doi.org/10.1016/j.procs.2020.10.075

Lukić, J., Radenković, M., Despotović-Zrakić, M., Labus, A., y Bogdanović, Z. (2016). A hybrid approach to building a multi-dimensional business intelligence system for electricity grid operators. Utilities Policy, 41, 95–106. https://doi.org/10.1016/j.jup.2016.06.010

Mall, S., y Saroj, S. K. (2018). A New Security Framework for Cloud Data. Procedia Computer Science, 143, 765–775. https://doi.org/10.1016/j.procs.2018.10.397

Polyvyanyy, A., Ouyang, C., Barros, A., y van der Aalst, W. M. P. (2017). Process querying: Enabling business intelligence through query-based process analytics. Decision Support Systems, 100, 41–56. https://doi.org/10.1016/j.dss.2017.04.011

Ramalingam, D., Arun, S., y Anbazhagan, N. (2018). A Novel Approach for Optimizing Governance, Risk management and Compliance for Enterprise Information security using DEMATEL and FoM. Procedia Computer Science, 134, 365–370. https://doi.org/10.1016/j.procs.2018.07.197

Sauerwein, C., Pekaric, I., Felderer, M., y Breu, R. (2019). An analysis and classification of public information security data sources used in research and practice. Computers and Security, 82, 140–155. https://doi.org/10.1016/j.cose.2018.12.011

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., y Klepacki, B. (2020). Information security assessment in public administration. Computers and Security, 90. https://doi.org/10.1016/j.cose.2019.101709

Vajirakachorn, T., y Chongwatpol, J. (2017). Application of business intelligence in the tourism industry: A case study of a local food festival in Thailand. Tourism Management Perspectives, 23, 75–86. https://doi.org/10.1016/j.tmp.2017.05.003

Wu, X., Zhang, R., Zeng, B., y Zhou, S. (2013). A trust evaluation model for cloud computing. Procedia Computer Science, 17, 1170–1177. https://doi.org/10.1016/j.procs.2013.05.149