Revista Especializada de Ingeniería
y Ciencias de la Tierra
VOL: 5 Nº 2 Enero - Junio 2026
ISSN L: 2805-1874

pp.64-81

La protección de datos de los bienes patrimoniales del Estado, Panamá 2024

The data protection of the patrimonial State assets, Panama 2024

Carlos A. Correa García De Paredes
Universidad de Panamá. Facultad de Ingeniería, Panamá
inquilino1969@gmail.com / carlos.correog@up.ac.pa
https://orcid.org/0009-0000-8207-4465

Santiago Y. García Díaz
Universidad de Panamá. Facultad de Ingeniería. Panamá
santiagogarciadiaz4822@gmail.com / santiago.garcia-d@up.ac.pa
https://orcid.org/0009-0003-1952-519X

Recibido: 9/10/2025 Aceptado: 31/10/2025

DOI https://doi.org/10.48204/reicit.v5n2.5838

RESUMEN

La investigación aborda la importancia de la protección de datos de los bienes patrimoniales estatales. Conviene mencionar que, para los países desarrollados, es un factor clave para salvaguardar los activos financiados con recursos públicos. En este contexto, el cibercrimen a la información de dichos bienes evidencia la urgencia de integrar un modelo robusto de protección de datos, como parte fundamental de la gestión patrimonial. La Contraloría General de la República de Panamá, conforme al Decreto Núm. 220-2014-DMySC del 25 de julio de 2014, publicado en la Gaceta Oficial Núm.27646 del 20 de octubre de 2014, adoptan las Normas Internacionales de Contabilidad del Sector Público (NICSP) en la República de Panamá. Asimismo, mediante el Decreto Núm.01-2017-DNMySC de 3 de enero de 2017, aprueba el Manual General de Contabilidad Gubernamental basado en las Normas Internacionales de Contabilidad del Sector Público (NICSP) - Versión II, publicado en la Gaceta Oficial No.28,198-A de 17 de noviembre de 2017. La implementación de las NICSP por parte de las entidades del sector público en Panamá es un proceso que requiere tiempo, recursos y compromiso de todas las partes involucradas. La adaptabilidad y la cooperación son esenciales para garantizar que se logren los objetivos de estandarización en el

pp.64-81

registro, transparencia, rendición de cuentas y buena gestión para la presentación de sus estados financieros, alineándose con las mejores prácticas internacionales. De acuerdo con el documento Instituciones del Sector Público, Panamá cuenta con 96 instituciones estatales que administran bienes patrimoniales. Este estudio analizó una muestra representativa de estas instituciones con el objetivo de evaluar un marco de seguridad para proteger la información patrimonial. Los resultados revelaron que el 66% de las instituciones evaluadas carecen de un plan integral de protección de datos en la gestión de sus bienes patrimoniales.

PALABRAS CLAVE: Protección de datos, Bienes patrimoniales del estado, Ciberseguridad

ABSTRACT

The research addresses the importance of data protection of state-owned assets. It is worth mentioning that, for developed countries, it is a key factor in safeguarding assets financed with public resources. In this context, cybercrime to the information of such assets shows the urgency of integrating a robust model of data protection as a fundamental part of asset management. The Office of the Comptroller General of the Republic of Panama, pursuant to Decree No. 220-2014-DMySC of July 25, 2014, published in the Official Gazette No.27646 of October 20, 2014, adopted the International Public Sector Accounting Standards (IPSAS) in the Republic of Panama. Likewise, through Decree No.01-2017-DNMySC of January 3, 2017, approves the General Governmental Accounting Manual based on the International Public Sector Accounting Standards (IPSAS) - Version II, published in Official Gazette No.28,198-A of November 17, 2017. The implementation of IPSAS by public sector entities in Panama is a process that requires time, resources and commitment from all parties involved. Adaptability and cooperation are essential to ensure that the objectives of standardization in recording, transparency, accountability, and good governance for the presentation of their financial statements are achieved, aligning with international best practices. According to the document Public Sector Institutions, Panama has ninety-six state institutions that manage assets. This study analyzed a representative sample of these institutions with the objective of evaluating a security framework to protect asset information. The results revealed that 66% of the institutions evaluated lack a comprehensive data protection plan for the management of their patrimonial assets.

KEYWORDS: Data protection, Patrimonial state assets, Cybersecurity

pp.64-81

INTRODUCCIÓN

La presente investigación aborda los siguientes términos, para una mejor comprensión:

- El control básico de los bienes patrimoniales consiste en la toma, registro y actualización de un inventario permanente, cuyo propósito es contar con información veraz y real entre los registros y el inventario; implementando controles efectivos que garanticen su existencia, estado de conservación y su debido uso. (Contraloría General de la República, 2017, p.24)
- **Bienes patrimoniales:** Son todos aquellos recursos materiales susceptibles de ser pesados, medidos, contados y verificados de propiedad del Estado. (Contraloría General de la República, 2017, p.117)
- **Controles internos:** Es un proceso integral efectuado por la Administración y el personal institucional, diseñado para enfrentarse a los riesgos y para dar una seguridad razonable de que, en la consecución de la misión de la entidad, se alcanzarán los objetivos generales (Contraloría General de la República, 2017, p.117)
- Por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa. (Ley No. 79, 22 de octubre de 2013, p. 16)
- Por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función. (Ley No. 79, 22 de octubre de 2013, p. 16)

Luego de estas definiciones, se observa la necesidad de proteger los datos informáticos que, representan todos los registros del patrimonio estatal, siendo esto un tema primordial para todas las instituciones que forman el Estado, por lo delicado y la responsabilidad que esto representa. En este mismo orden de ideas, se destaca otros conceptos, los cuales involucran la protección de la información contra los ciberataques, por tanto:

> La ciencia de datos ha ganado relevancia en los procesos investigativos porque permite apoyarlos, mejorar la toma de decisiones y así: dar respuesta a preguntas mediante la información que las organizaciones recolectan – por ejemplo, en los *Security Information and Event Management (SIEM)*–, la cual representa el contexto de un incidente informático: ¿cuándo?, ¿dónde?, ¿quién?,

> ¿por qué?; y crear mecanismos para la prevención, detección y respuesta a eventos delictivos. (Urcuqui López, C.; Navarro Cadavid, A. Coordinadores, 2022, pp.9-10)

Según Martínez et al.,(2024), Hoy en día, los ciberataques se han convertido en una forma de robo muy común debido a los avances en la tecnología y los procesos de internet en las empresas, organizaciones y principalmente bancos, infiltrándose directamente en la seguridad de todo tipo de corporaciones en Panamá y el mundo; y Panamá es uno de los países más vulnerables para los ciberdelincuentes.

Según estudio de mercado realizado por la embajada de España en Panamá, nos cuenta una descripción clara de la estructura en materia de comunicación de Panamá:

> Con alrededor de cuatro millones de habitantes, Panamá tiene una tasa de penetración de Internet relativamente alta de 2,9 millones, o el 67 % de la población 2. Cerca de 2,5 millones de panameños obtienen acceso a internet a través de sus teléfonos inteligentes. Panamá cuenta con las mejores conexiones de fibra óptica submarina de América Latina, con conectividad a ocho cables submarinos. El país está cableado en las costas del Pacífico y del Atlántico, y está conectado directamente con muchos países del hemisferio occidental: América del Norte, América del Sur, América Central y el Caribe.(Blanco, 2022, p. 5)

Dentro del marco de la investigación sobre la protección de los datos, los autores Arroyo Guardeño, Gayoso Martínez y Hernández Encinas (2020) plantean:

> La disciplina de la seguridad se encarga de proteger los activos de una organización o de un particular. Un activo es cualquier elemento que tiene valor para una organización o sujeto. En general la seguridad de la información abarca todo aquello que tiene que ver con la protección de la información, ya sea almacenada o trasmitida. Cuando la información se trasmite, entonces se hace referencia a la seguridad TIC, en el sentido que son las tecnologías de la información y las comunicaciones las encargadas de velar por los activos. Por su parte, la ciberseguridad no solo contempla la seguridad de información que se trasmite (momento en el que se interseca con la seguridad de la información), sino que contempla otros activos que no son solo información, pero que también pueden ser atacados por la TIC.
>
> La protección de los activos se realiza frente a la acción de los atacantes. Debe tenerse en cuenta que el objetivo de un atacante suele ser el de explotar las debilidades asociadas a cualquier dispositivo que esté a su alcance (ordenador, teléfono, tableta, etc.) con el fin de sacar provecho a la vulneración de cualquiera de los tres objetivos principales relacionados con la seguridad de un sistema informático: confidencialidad, integridad y disponibilidad (CID).La confidencialidad

> garantiza la protección de la información de modo que sea secreta para quienes no tienen derecho a acceder a la misma. La integridad asegura la autenticidad de los datos almacenados, de modo que no puedan ser modificados, manipulados ni alterados por terceras partes sin permiso para ello. Finalmente, la disponibilidad de los datos almacenados en un sistema informático obliga a que su acceso sea posible en cualquier momento que sea solicitado por cualquier parte que esté autorizada a ello. (pp.15-16)

Cabe ampliar lo anterior, con las aportaciones realizadas por el autor Rea Guamán (2020), en su tesis doctoral "Madurez en la Identificación y Evaluación de Riesgos en Ciberseguridad", de la Universidad Politécnica de Madrid, cuando sostiene que:

> Los ataques cibernéticos comprometen la confidencialidad robando datos, comprometiendo la integridad mediante la modificación de datos o comprometiendo la disponibilidad al negar acceso a datos, servicios o sistemas.

Los ataques de integridad implican la modificación de datos, lo que puede dar lugar a diversos impactos que incluyen lo siguiente:

- Impactos reputacionales si esos datos son información pública como sitios web.
- Impactos de la información financiera si se trata de datos financieros, particularmente para una corporación que cotiza en bolsa.
- Pérdidas de dinero real si los datos que se cambian son números de enrutamiento bancario o mandatos financieros a los bancos que manejan cuentas corporativas.
- Disponibilidad: denegar acceso.

El tercer tipo de ciberataque es afectar la disponibilidad de los sistemas y denegar el acceso a ello. Los ataques que causan la denegación de servicios pueden ser difíciles de diagnosticar, especialmente si los sistemas están dañados, pero no deshabilitados. A menudo, los sistemas se deterioran cuando el ataque causa fallos abrumadores a los sistemas y la infraestructura. (2020, pp.10-12)

Estos, han motivado a los gobiernos, a hacer frente a tal circunstancia, aportando respuestas expeditas, que faciliten la protección de sus usuarios, ya sean empresas como particulares, a través de regulaciones las cuales desde hace mucho tiempo se han tratado de unificar para que exista una misma normativa en todos los países. (p.15).

Dentro del marco regulatorio en Panamá, se tiene el Código Penal de la República de Panamá, en su Título VIII los "Delitos contra la Seguridad Jurídica de los Medios Electrónicos", en el Capítulo I Delitos

contra la Seguridad Informática, normativa aprobada mediante la Ley 14 del 18 de mayo de 2007, encontramos los artículos:

> **Artículo 289.** Quien indebidamente ingrese o utilice una base de datos, red o sistema informático será sancionado con dos a cuatro años de prisión.
>
> **Artículo 290.** Quien indebidamente se apodere, copie, utilice o modifique los datos en tránsito o contenidos en una base de datos o sistema informático, o interfiera, intercepte, obstaculice o impida su transmisión será sancionado con dos a cuatro años de prisión.
>
> **Artículo 291.** Las conductas descritas en los artículos 289 y 290 se agravarán de un tercio a una sexta parte de la pena si se cometen contra datos contenidos en bases de datos o sistema informático de:
>
> 1. Oficinas públicas o bajo su tutela.
> 2. Instituciones públicas, privadas o mixtas que prestan un servicio público.
> 3. Bancos, aseguradoras y demás instituciones financieras y bursátiles.
>
> También se agravará la pena en la forma prevista en este artículo cuando los hechos sean cometidos con fines lucrativos.
>
> Estas sanciones se aplicarán sin perjuicio de las sanciones aplicables si los datos de que trata el presente Capítulo consisten en información confidencial de acceso restringido, referente a la seguridad del Estado, según lo dispuesto en el Capítulo I, Título XIV, del Libro Segundo de este Código.
>
> **Artículo 292.** Si las conductas descritas en el presente Capítulo las comete la persona encargada o responsable de la base o del sistema informático, o la persona autorizada para acceder a este, o las cometió utilizando información privilegiada, la sanción se agravará entre una sexta y una tercera parte. (Código Penal de la República de Panamá, 2016, p. 212)

La República de Panamá, mediante la Ley No. 79 de 22 de octubre de 2013, publicada en la Gaceta Oficial No.27403-A del 25 de octubre de 2013, aprobó el Convenio sobre la Ciberdelincuencia, hecho en Budapest, el 23 de noviembre de 2001.

Otra cuestión importante en Panamá es la existencia de entidades con responsabilidades de perseguir o prevenir los delitos de ciberseguridad, como: La Fiscalía Especializada en Delitos Contra la Propiedad Intelectual y Seguridad Informática en el Ministerio Público. El Centro Nacional de Respuestas de

Incidentes de Seguridad de la Información de Panamá (CSIRT Panamá), que "entre sus objetivos están la prevención, tratamiento, identificación y resolución de ataques a incidentes de seguridad sobre los sistemas informáticos que conforman la infraestructura crítica del país y el acceso a la información de parte de los ciudadanos de Panamá." (CSIRT, 2023, Sobre nosotros). La Policía Nacional de Panamá. La Autoridad Nacional para la Innovación Gubernamental (AIG) que, a través de su Consejo Nacional para la Innovación Gubernamental, aprobó la Resolución No.17 del10 de septiembre de 2021, que establece la Estrategia Nacional de Ciberseguridad para el periodo 2021-2024, la cual consta de cuatro (4) pilares, el Pilar 1-Proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio. Pilar II- Disuadir y castigar el comportamiento criminal en el ciberespacio. Pilar III-Fortalecer la seguridad y la resiliencia de la infraestructura critica de nuestra nación. Pilar IV-Fomentar una cultura nacional de ciberseguridad. Igualmente, existe la Campaña Nacional "Panamá Ciberseguridad", con la misión de promover la comunidad panameña, el conocimiento en ciberseguridad; y con el objetivo de fomentar una cultura nacional de ciberseguridad, entendiéndola que es una responsabilidad de todos.

MATERIALES Y MÉTODOS

> La investigación aplicada, concentra su atención en las posibilidades concretas de llevar a la práctica las teorías generales, y destina sus esfuerzos a resolver las necesidades que se plantean la sociedad y los hombres.
>
> La resolución de problemas prácticos se circunscribe a lo inmediato, por lo cual su resultado no es aplicable a otras situaciones. (Baena Paz, 2017, p.18)

Enfoque cuantitativo

El más conocido de los enfoques, el cuantitativo utiliza la recolección y análisis e interpretación de los datos para contestar preguntas de investigación o probar hipótesis establecidas previamente. Este enfoque está fundamentado en la medición numérica, el conteo de los datos y la utilización de estadística para establecer con exactitud los factores de comportamiento en una población o muestra. Utiliza las variables para la recolección de los datos. Es deductivo, objetivo, medible y comprobable. (Maldonado Pinto, 2018, p.35)

Esta investigación es tipo aplicado y de enfoque cuantitativo, que busca describir, detallar y exponer una situación real, según una población o grupo de participantes que corresponde al sector público con noventa y seis (96) instituciones estatales en Panamá, que se encargan de administrar sus bienes patrimoniales. La Contraloría General de la República (2017), en el *Manual de normas generales y*

procedimientos para la administración y control de los bienes patrimoniales (activos fijos e intangibles y bienes no depreciables) en el sector público, tomos I y II, segunda versión, establece que: *"*Cada entidad tiene que practicar anualmente, inventarios físicos de los bienes de su propiedad, bajo su administración, uso y custodia, con el objeto de verificar su existencia física y estado de conservación" (p.24). Al mismo tiempo, plantea el control básico de los bienes patrimoniales, **¿en qué consiste?** "en la toma, registro y actualización de un inventario permanente" (p.24), **¿cuál es el propósito?** "contar con información veraz y real entre los registros y el inventario" (p.24) **¿cómo?** "implementando controles efectivos que garanticen su existencia, estado de conservación y su debido uso" (p.24).Este Manual se aplicará en lo relativo al uso y manejo de los Bienes Patrimoniales, en el: "Gobierno General, Gobierno Locales (Municipios, Juntas Comunales), Proyectos de Inversión, Instituciones sin fines de lucro (Patronatos), Corporaciones Públicas no financieras (Empresas Públicas, Corporaciones y Proyectos de Desarrollo), Corporaciones Públicas Financieras (Intermediarios Financieros), y el Servicio Exterior" (2017, p.16).

Para obtener los resultados, se empleó la técnica de encuesta con una muestra significativa de las respuestas de 40 colaboradores vinculados a los bienes patrimoniales de instituciones públicas, que representa 41% del total de 96 entidades, como se muestra en la Tabla 1. Se utilizó un cuestionario para la recolección de datos con tecnología de inteligencia artificial, de la plataforma Microsoft Forms, para visualizar en gráfico y tiempo real las respuestas de 15 preguntas. El cuestionario en línea se abrió del 11 al 17 de septiembre de 2024. Para obtener las respuestas de los colaboradores relacionadas con los bienes patrimoniales de las entidades encuestadas, nos contactamos con personal del Ministerio de Economía y Finanzas, que nos facilitaron los teléfonos de contacto de dicho personal. Los Gobiernos Locales aun cuando les aplica el Manual de uso y manejo de los Bienes Patrimoniales, no fueron incluidos en la Tabla 1.

Tabla 1.

Categoría de entidades estatales

#	Entidades	Cantidad
1	Gobierno Central	30
2	Instituciones Descentralizadas	42
3	Empresas Públicas	16
4	Intermediarios Financieros	8

Revista Especializada de Ingeniería y Ciencias de la Tierra
VOL: 5 Nº 2 Enero - Junio 2026
ISSN L: 2805-1874
pp.64-81

Total	96

Nota: Se muestra en la Tabla 1 la cantidad de entidades estatales según categorizaciones. Se elaboro a partir del Informe de Planilla del Sector Público al 31 de julio de 2024 de la Contraloría General de la República de Panamá.

RESULTADOS

Figura 1.

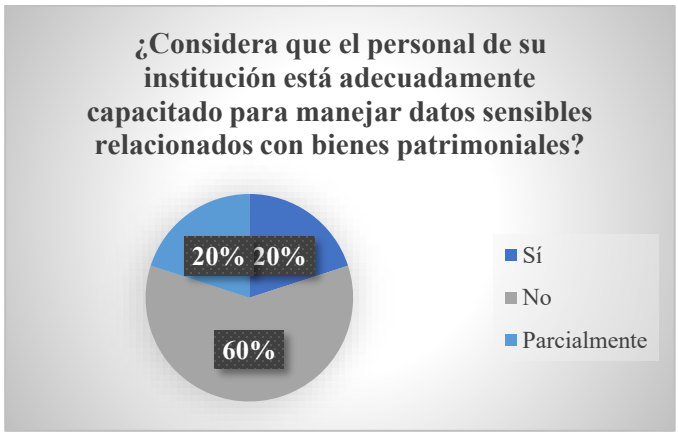
Implementación de un plan de protección de datos

Nota: La Figura 1 muestra que, 70% de los encuestados indican que sus organizaciones no cuentan con un plan establecido, reflejando una notable carencia en la implementación de medidas estructuradas para la protección de datos. El 30% indica que sí tienen un plan formal en funcionamiento. Aunque algunas instituciones están tomando medidas proactivas, la mayoría aún no adopta estrategias formales de protección. Esta brecha sugiere la necesidad urgente de desarrollar y formalizar políticas y planes en garantía de la seguridad de los datos e información patrimonial sensible en el entorno digital.

Figura 2.

Personal capacitado en manejo de datos de bienes patrimoniales

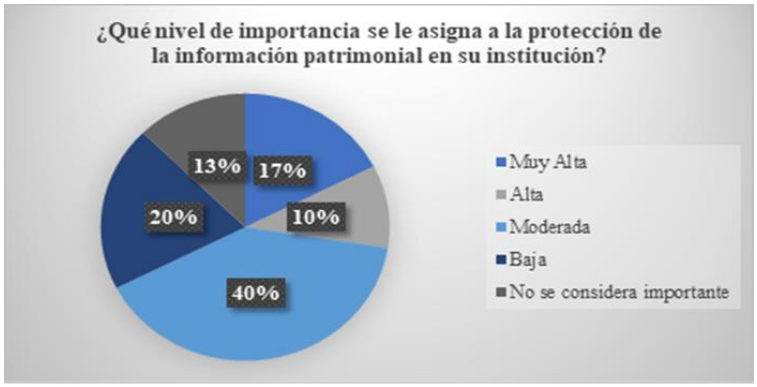
pp.64-81



Nota: La Figura 2 presenta un panorama preocupante. El 20% de los encuestados considera que el personal de su institución está adecuadamente capacitado, el 60% que no lo está, el 20% que está parcialmente capacitado. Los resultados advierten que, una mayoría significativa de las entidades carece de la formación necesaria en el manejo de información crítica de manera segura y efectiva, situación que expone a riesgos la gestión de bienes patrimoniales. La falta de capacitación adecuada acentúa la necesidad de implementar programas de formación más robustos y continuos para asegurar la protección de los datos institucionales.

Figura 3.

Importancia de la protección de la información patrimonial



Nota: En la Figura 3 se muestra la percepción mixta de la importancia de la protección de la información patrimonial en las instituciones. Solo 17% lo considera como de "muy alta" prioridad, 10% de importancia "alta.", 40% que la importancia es "moderada", revelando que, aun cuando las entidades reconocen su relevancia, no se le otorga el valor para garantizar

una protección robusta. Inquietante, el 20% de las respuestas indica que la protección de la información patrimonial tiene una importancia "baja" o "no se considera importante." Los resultados apuntan a la necesidad de concienciar y priorizar la seguridad de la información patrimonial en muchas instituciones, dada la creciente amenaza de ciberataques y el valor estratégico que la información tiene en la continuidad y estabilidad operativa.

Figura 4.

Políticas de la privacidad de datos en la información patrimonial

Nota: La Figura 4 muestra que un porcentaje significativo de las instituciones carece de políticas específicas de privacidad de datos para proteger la información patrimonial. El 52% señala que su institución no tiene estas políticas, lo que evidencia no gestiona la seguridad de la información, el 25% afirma tener políticas específicas, y el 23 % que están desarrollando en sus instituciones, lo que resalta que algunas entidades reconocen la necesidad de mejorar sus marcos normativos en torno a la privacidad de datos.

CONCLUSIONES

En primer lugar, con relación a la pregunta **1. Tipo de institución**, se puede indicar que, de 96 instituciones, se logró las respuestas de cuarenta (40) instituciones. En el cual, dieciocho (18) son ministerios y representan de la encuesta el 45%; catorce (14) fueron entidades autónomas o semiautónomas, representando el 35%; cinco (5) empresas estatales, representando el 13%; y tres (3) que pertenece a otro tipo de institución estatal, representando el 8% de la encuesta.

Teniendo en cuenta, la pregunta **2. Número aproximado de empleados en su institución.** Diecinueve instituciones indicaron que tiene una media de 100 a 500 empleados, el 48% de la encuesta; quince (15) instituciones con un promedio mayor de 500 empleados, el 38%; y se destaca que seis (6) instituciones tienen un promedio de menos 100 empleados, el 15 % de la encuesta. Lo que representa que la mayoría de los encuestados son entidades medianas y el promedio de entidades grandes representa un 38%.
Como resultado a la pregunta 3. **¿Qué tipo de bienes patrimoniales administra su institución?**, treinta y cuatro (34) respondieron bienes muebles e inmuebles, representando el 85% de la encuesta; dos (2) respondieron inmuebles, dos (2) contestaron bienes muebles y dos (2) señalaron que otros, lo que representan cada grupo un 5% de la encuesta. Esto demuestra que la mayoría de las entidades manejan propiedad, planta y equipo, es decir casi todos los bienes y un porcentaje menor otro tipo de bienes, cómo culturales, semovientes y otros que entran en otras categorías.

En la pregunta **4. ¿Su institución tiene implementado un plan formal de protección de datos para la gestión de bienes patrimoniales?** La encuesta revela que el 70% de las instituciones no tiene un plan formal de protección de datos para gestionar bienes patrimoniales, lo que indica una grave deficiencia al implementar medidas de seguridad estructuradas. Solo el 30% ha establecido un plan, lo que sugiere que, aunque algunas organizaciones están avanzando en la protección de datos, la mayoría aún carece de estrategias formales. Esta situación resalta la necesidad urgente de crear y formalizar políticas que garanticen la seguridad de la información sensible en un entorno digital cada vez más crítico.

Se observa en la pregunta **5. ¿Qué nivel de importancia se le asigna a la protección de la información patrimonial en su institución?** Esto indica que, según los resultados arrojados, un 42% considera moderado, si existe protección, pero no está claro en este tema, ya que en otra respuesta se manifestó que se percibe una complejidad en la gestión de bienes patrimoniales, lo que nos lleva a capacitar, concientizar a los encargados de llevar los patrimoniales estatales, su importancia y relevancia.

Por otra parte, en la pregunta **6. ¿Su institución ha sido víctima de un ciberataque o filtración de datos en los últimos 5 años?**, La encuesta revela que el 50% de las instituciones ha sido víctima de un ciberataque o filtración de datos en los últimos cinco años, lo que indica que la ciberseguridad es una preocupación significativa para la mitad de las organizaciones. Esto enfatiza la urgencia de fortalecer las medidas de protección y respuesta ante incidentes de seguridad.

En consideración a lapregunta**7. ¿Cuenta su institución con políticas específicas de privacidad de datos para la protección de la información patrimonial?** Según la respuesta, podemos concluir que la mayoría de las entidades encuestadas no cuentan con políticas específicas de privacidad, donde podemos indicar que la mayoría de las entidades están expuestas a un ciberataque en la gestión de la data de su patrimonio.

Cabe mencionar, en la pregunta **8. ¿Qué tipo de tecnologías o software utiliza su institución para proteger los datos patrimoniales?** (seleccione los tres más relevantes). La encuesta revela que las instituciones priorizan las copias de seguridad automatizadas y los firewalls como tecnologías clave para proteger los datos patrimoniales, seguidas por los sistemas de detección de intrusos y sistemas de cifrado. Sin embargo, la diversidad en las respuestas bajo la categoría de otros sugiere la existencia de múltiples enfoques en la implementación de tecnologías de seguridad. Estos hallazgos subrayan la necesidad de fortalecer y diversificar las estrategias de protección de datos en las instituciones.

Por otro lado, en la pregunta **9. ¿Su institución está alineada con las Normas Internacionales de Contabilidad del Sector Público (NICSP) en cuanto a la gestión de bienes patrimoniales?,** Aquí podemos concluir la necesidad de incrementar la implementación de las Normas NICSP a nivel nacional, considerando que dicho proceso se está realizando poco a poco. La debida implementación es significativa para la contabilidad y finanzas del sector público panameño, valorando que las mismas constituye el marco regulatorio y estandarizado, lo que contribuye al mantenimiento de estados contables sólidos, con datos e información financiera transparente, sobre todo en beneficio de la gestión patrimonial.

Tal y como se muestra en la pregunta **10. ¿Qué marco regulatorio sigue su institución en términos de privacidad y protección de datos?** Los resultados de la Figura 10, destacan la necesidad urgente de

establecer políticas efectivas y mejorar la capacitación para fortalecer la gestión de la información patrimonial. Teniendo en cuenta estos resultados, es útil reiterar que, en la República de Panamá, existe un marco regulatorio vigente, como la Ley 14 del 18 de mayo de 2007, que establece en el Código Penal los normas sobre "Delitos contra la Seguridad Informática"; la Ley No. 79 de 22 de octubre de 2013, que aprobó el Convenio sobre la Ciberdelincuencia; la Resolución No. 17 de 10 de septiembre de 2021 del Consejo Nacional para la Innovación Gubernamental, por la cual se aprueba la Estrategia Nacional de Ciberseguridad para el periodo 2021-2024; la Campaña Nacional "Panamá Ciberseguridad"; así como distintas normativas de protección de datos.

Conviene destacar en la pregunta **11. ¿Su institución ofrece capacitaciones regulares sobre privacidad y protección de datos a sus empleados?** En la Figura 3 se destaca que un 30% de las entidades encuestadas no ofrecen capacitación sobre el tema de privacidad y protección de datos, por consiguiente, es relevante para las entidades como, la Autoridad Nacional para la Innovación Gubernamental (AIG), la Dirección General de Carrera Administrativa, el Ministerio de Economía y Finanzas, la Contraloría General de la República, entre otras, fomentar la sinergia para establecer metas y objetivos comunes, para la formación y capacitación de los servidores públicos, respecto a la protección de datos de los bienes patrimoniales en las distintas instituciones del Estado Panameño.

Cabe distinguir en la **pregunta 12. ¿Considera que el personal de su institución está adecuadamente capacitado para manejar datos sensibles relacionados con bienes patrimoniales?** Como se indicó en la Figura 4, los resultados sugieren que una mayoría significativa de las instituciones carece de la formación necesaria para manejar información crítica de manera segura y efectiva, lo que podría exponer a riesgos importantes la gestión de bienes patrimoniales. A nivel institucional, es primordial establecer programas de formación para los servidores públicos, con énfasis en el manejo, privacidad y protección de datos e información de los bienes patrimoniales estatales, a fin de promover la cultura de ciberseguridad en la gestión pública, en concordancia con la "Estrategia Nacional de Seguridad" para el periodo 2021-2024 en Panamá.

Como resultado de la pregunta **13. ¿Cuáles son los mayores desafíos que enfrenta su institución en la protección de datos patrimoniales?** (seleccione los tres más relevantes), Los principales desafíos en la protección de datos patrimoniales son la ausencia de políticas claras, la complejidad en la gestión de

bienes y la insuficiente capacitación del personal. Estos hallazgos subrayan la necesidad urgente de implementar políticas efectivas y mejorar la formación del personal para optimizar la protección y gestión de la información patrimonial en las instituciones.

Respecto a los resultados de la pregunta **14. ¿Qué acciones considera prioritarias para mejorar la privacidad y protección de datos en su institución?**, Los resultados de la Figura 5, nos enfatizan lo esencial de establecer medidas orientadas a la protección de los datos. Por eso, entre las acciones que se pueden implementar, para mejorar la privacidad y protección de los datos e información, en relación con los bienes patrimoniales estatales, consideramos fundamental, primero, evaluar los riesgos afines al manejo de dicha información, para identificar debilidades, posibles amenazas y cualquier vulnerabilidad del sistema o de los procesos de la gestión patrimonial. Es imprescindible adoptar regulaciones de ciberseguridad, establecer políticas y procesos claros; disponer de tecnologías que refuercen la protección y privacidad de la información; realizar las auditorias de seguridad o la que corresponda, y sus debidos seguimientos. Al mismo tiempo que el desarrollo de estas actividades es imperioso, instaurar un programa de capacitación para el personal vinculado a la administración de los bienes, valorando que el recurso humano es indispensable, en el éxito de toda buena gestión sobre la protección y privacidad de la información.

Hay que mencionar en referencia a la pregunta **15. En una escala de 1 a 5, donde 1 es muy baja y 5 es muy alta, ¿cómo evalúa el nivel actual de seguridad en la protección de la información patrimonial en su institución?**, La percepción de las medidas de seguridad es mayoritariamente negativa, con el 45% de los encuestados calificándolas como insuficientes y solo un 23% considerándolas efectivas. Esto destaca una necesidad urgente de fortalecer y mejorar las estrategias de seguridad en la mayoría de las instituciones para garantizar una protección adecuada de sus datos.

Tras realizar este estudio y analizar las respuestas obtenidas, la investigación corrobora que, la mayoría de las entidades estatales carecen de un sistema adecuado para proteger los datos en la gestión de bienes patrimoniales. Además, las entidades muestran desinformación y falencia en relación con el manejo de dichos datos, debido a la complejidad que esto representa. La muestra representativa utilizada demostró la necesidad de capacitar al personal encargado de la gestión de bienes patrimoniales estatales. Los temas concernientes a la protección de datos han alcanzado gran relevancia a nivel global, y, por otra parte, es

imperativo implementar las Normas Internacionales de Contabilidad del Sector Público (NICSP), para estandarizar los registros y la presentación de los estados financieros gubernamentales, contribuyendo así al desarrollo económico de los países y Panamá.

Observación: Para aquellos lectores que deseen profundizar en los temas tratados en este artículo o recibir asesoría personalizada, les invitamos a ponerse en contacto con los autores. Estaremos encantados de ofrecer apoyo adicional y responder a cualquier consulta relacionada con el contenido presentado.

REFERENCIAS BILIOGRÁFICAS

Arroyo Guardeño, D.; Gayoso Martínez, V.; Hernández Encinas, L. *Ciberseguridad*. Ed. Madrid: Editorial CSIC Consejo Superior de Investigaciones Científicas, 2020. 144 p. https://elibro.net/es/ereader/upanama/172144?as_all=protecci%C3%B3n__de__datos&as_all_op=unaccent__icontains&fs_page=3&prev=as

Baena Paz, G.M.E. Metodología de la investigación. ed. México, D.F.: Grupo Editorial Patria, 2017. 157 p. https://elibro.net/es/ereader/upanama/40513?as_all=metodolog%C3%ADa&as_all_op=unaccent__icontains&prev=as

Blanco, L. (2022). El mercado de la ciberseguridad en Panamá [Estudio de Mercado]. https://www.icex.es/content/dam/es/icex/oficinas/092/documentos/2022/10/documentos-anexos/DOC2022915843.pdf

Checkpoint. (2024). What is the CIA Triad? https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-it-security/what-is-the-cia-triad/

Código Penal de la República de Panamá (Texto Único comentado) Adoptado por la Ley 14 de 2007 (publicada el 22 de mayo de 2007, Gaceta Oficial No. 25796), Panamá: Ministerio Público, Procuraduría General de la Nación. 322p.

Contraloría General de la República. (5 de mayo de 2017). Decreto No. 32-2017-DMySC. *Por el cual se aprueba el "Manual de normas generales y procedimientos para la administración y control de los bienes patrimoniales (activos fijos e intangibles y bienes no depreciables) en el sector público, tomos I y II, segunda versión"*. Panamá, Panamá. Obtenido de https://vlex.com.pa/vid/decreto-n-32-2017-905411851

Contraloría General de la República de Panamá. Informe de Planilla del Sector Público al 31 de julio de 2024. Agosto 2024. 36p.

https://www.contraloria.gob.pa/wp- content/uploads/2024/09/Informe-Planilla-del-Sector-Publico-Julio-2024.pdf

Correa García de Paredes, C.A. (2024). Importancia de la Implementación de un Sistema Integrado de Gestión para la Optimización de los Procesos de los Bienes Patrimoniales de la Universidad de Panamá, 2024.Revista Especializada de Ingeniería y Ciencias de la Tierra, Volumen 3 No.2 enero – junio 2024. pp.183-197. https://revistas.up.ac.pa/index.php/REICIT/article/view/4688

CSIRT (Computer Security Incident Response Team). 2023. Sobre nosotros. https://cert.pa/?page_id=33

Fortinet. (2024). Tríada CIA: confidencialidad, integridad y disponibilidad. https://www.fortinet.com/lat/resources/cyberglossary/cia-triad

Godoy Troya (2021). Impacto en los Sistemas de Información Contable por Efecto de los Delitos Informáticos a las Operaciones de Banca por Internet en la Ciudad de Panamá.Tesis de Doctorado. Universidad de Panamá. Panamá. 255p.

Rea Guamán, A.M. Madurez en la Identificación y Evaluación de Riesgos en Ciberseguridad. Tesis de Doctorado.Universidad Politécnica de Madrid. Madrid. 2020. 446p. https://oa.upm.es/65871/1/ANGEL_MARCELO_REA_GUAMAN.pd

Ley No. 79 (22 de octubre de 2013), La Asamblea Nacional de Panamá aprobó el Convenio sobre la Ciberdelincuencia. 25 de octubre de de 2013. Gaceta Oficial Digital No. 27403-A.

Maldonado Pinto, J.E. Metodología de la investigación social: paradigmas: cuantitativo, sociocrítico, cualitativo, complementario. ed. Bogotá: Ediciones de la U, 2018. 297p. https://elibro.net/es/ereader/upanama/70335?as_all=metodolog%C3%ADa__cuantitativa&as_all_op=unaccent__icontains&prev=as

Martínez, Y., Cerezo, J., & Quirós, A. (2024). ¿Cómo el ciberdelito afecta a las empresas e instituciones bancarias en Panamá? https://revistas.umecit.edu.pa/index.php/sc/article/download/1380/2262/8650

Oficina Económica y Comercial de la Embajada de España en Panamá. (2022). El mercado de la ciberseguridad en Panamá [Estudio de Mercado]. https://www.icex.es/content/dam/es/icex/oficinas/092/documentos/2022/10/documentos-anexos/DOC2022915843.pdf

Panamá Cibersegura. 2023. https://panamacibersegura.gob.pa/index.php/nosotros/

Resolución No.17 (10 de septiembre de 2021). El Consejo Nacional para la Innovación Gubernamental aprueba la Estrategia Nacional de Ciberseguridad para el periodo 2021-2024. 15 de diciembre de 2021. Publicada en la Gaceta Oficial Digital No. 29434-A. https://www.gacetaoficial.gob.pa/pdfTemp/29434_A/GacetaNo_29434a_20211215.pdf

Urcuqui López, C.C.; Navarro Cadavid, A. (Coordinadores). Ciberseguridad: Los datos tienen la respuesta. Cali: Editorial Universidad Icesi, 2022. 274 p. https://elibro.net/es/ereader/upanama/225844?as_all=ciberseguridad&as_all_op=unBlanco, L. (2022).