Revista del Archivo General de la Nación 2025; 40(1); 87-116

Diagnóstico de implementación de sistemas de gestión de seguridad de la información en los archivos generales nacionales de Latinoamérica según la ISO/IEC 27001

María José Bravo Ramos[1]

Resumen

Este estudio examina la implementación de sistemas de gestión de seguridad de la información en los archivos generales nacionales de Latinoamérica en base a las recomendaciones de la norma ISO/IEC 27001, con el fin de conocer los métodos actuales de protección, identificar posibles áreas de mejora y determinar estrategias que garanticen la defensa de sus activos de información. Se utilizó una investigación de carácter cuantitativo por medio de la técnica de muestreo probabilístico estratificado, basada en una población de 16 instituciones archivísticas asociadas a la Asociación Latinoamericana de Archivos. Para recolectar los datos, se elaboró una encuesta dirigida a los directores de los archivos generales nacionales, con la que se obtuvo una tasa de respuesta del 68,75 %, equivalente a 11 respuestas. Los resultados demuestran que la gran parte de estos archivos han implementado prácticas básicas de seguridad, tales como copias de seguridad, controles de acceso físico y políticas institucionales. No obstante, se localizaron debilidades en la adopción de intervenciones de seguridad más sofisticadas, como el uso del cifrado y la biometría, la estandarización de procedimientos de eliminación segura, la capacitación continua de los archivistas, y la gestión de riesgos. La simultaneidad de soportes analógicos y electrónicos, junto con tecnologías obsoletas, demuestra la urgencia de renovar la infraestructura tecnológica y definir planes de preservación digital. En síntesis, aunque se ha concientizado sobre la importancia de asegurar la información, la implementación de los SGSI en los archivos aún es limitada. Es indispensable fortalecerla a través de la adopción de estándares internacionales, la formación constante del personal, la cooperación entre

1 Doctora por la Universidad Carlos III de Madrid y docente en la Universidad Técnica de Manabí (Ecuador). ORCID: 0000-0001-9220-3451. Correo electrónico: maria.bravo@utm.edu.ec.

Citar como: Diagnóstico de implementación de sistemas de gestión de seguridad de la información en los archivos generales nacionales de Latinoamérica según la ISO/IEC 27001. *Revista del Archivo General de la Nación*, 40(1), 87-116. DOI: 10.37840/ragn.v40i1.182

Recibido: 14/09/2025. Aprobado: 03/02/2026. En línea: 12/06/2026..

países de la región y la modernización de infraestructuras tecnológicas. Estas prácticas contribuirán a salvaguardar la memoria histórica latinoamericana de forma integral y garantizar su continuidad digital para las generaciones futuras.

Palabras clave: ISO/IEC 27001, Sistema de Gestión de Seguridad de la Información, Archivos Generales Nacionales, Latinoamérica.

Assessment of implementation of Information Security Management Systems in Latin American national general archives according to ISO/IEC 27001

Abstract

This study focuses on examining the implementation of information security management systems in the national archives of Latin America according to the recommendations of the ISO/IEC 27001 standard, with the aim of understanding current protection methods, identifying possible areas for improvement, and determining strategies that guarantee the defense of their information assets. Quantitative research was used, employing a stratified probability sampling technique based on a population of 16 archival entities associated with the Latin American Association of Archives. To collect the data, a survey was conducted among the directors of national archives, with a response rate of 68,75 %, equivalent to 11 responses. The results show that most of these archives have implemented basic security practices, such as backups, physical access controls, and institutional policies. However, weaknesses were identified in the adoption of more sophisticated security controls, such as the use of encryption and biometrics, the standardization of secure disposal procedures, the ongoing training of archivists, and risk management. The simultaneous use of analog and electronic media, together with obsolete technologies, demonstrates the urgency of renewing the technological infrastructure and defining digital preservation plans. In summary, although awareness of the importance of securing information has grown, the implementation of ISMSs in archives is still limited. It is essential to strengthen this through the adoption of international standards, ongoing staff training, cooperation between countries in the region, and the modernization of technological infrastructure. These practices will contribute to safeguarding Latin America's historical memory in a comprehensive manner and ensuring its digital continuity for future generations.

Keywords: ISO/IEC 27001, Information Security Management System, National General Archives, Latin America.

Introducción

Los archivos han sido hasta nuestros días custodios de la memoria de los pueblos, constituyen una fuente para la defensa de sus derechos y son sedes de investigaciones

históricas, políticas y culturales porque permiten comprender el pasado, construir el presente y orientar el futuro. Por lo tanto, los archivos históricos son una herramienta fundamental en la preservación de la memoria, la investigación, la educación, la toma de decisiones, la transparencia, la rendición de cuentas y la protección de los derechos.

Hoy en día, los avances tecnológicos ofrecen la posibilidad de automatizar los procesos del archivo y mejorar sus procesos de descripción archivística, promoviendo consultas más rápidas y accesibles para todos los usuarios interesados. Sin embargo, estas innovaciones tecnológicas exponen a la información custodiada a nuevas amenazas en el entorno digital, como ciberataques, almacenamiento inadecuado, vulneraciones en el acceso, falta de políticas de preservación digital de la memoria, obsolescencia de los soportes, falta de copias de seguridad de la información, pérdida accidental o intencional de datos, falta de capacitación en la gestión de seguridad de la información y ausencia de planes de contingencia.

Ante esta realidad, es indispensable adoptar medidas de seguridad a fin de evitar los referidos incidentes y garantizar una adecuada gestión de riesgos. En este marco, la seguridad de la información desempeña un rol fundamental como un conjunto de medidas preventivas y reactivas necesarias en las organizaciones para salvaguardar la información, independientemente del soporte, asegurando la confidencialidad, integridad y disponibilidad de la misma y permitiendo su accesibilidad a largo plazo.

Con el propósito de que las instituciones puedan cumplir eficazmente el objetivo de proteger sus activos de información, se han desarrollado diversas normas internacionales, entre las que destacan la familia de normas ISO/IEC 27000 y la ISO 16363, ampliamente reconocidas en el ámbito de la seguridad y preservación de la información. En particular, la norma ISO/IEC 27001, como parte de la familia ISO/IEC 27000, establece un marco de referencia internacional orientado a la gestión de la seguridad de la información mediante la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

El objetivo principal de un SGSI es proporcionar un marco sistemático y documentado que permita a las organizaciones proteger la confidencialidad, integridad y disponibilidad de la información, gestionando de manera eficaz los riesgos asociados a su tratamiento. Este sistema no se limita a la aplicación de controles técnicos, sino que integra políticas, procesos, roles organizativos y mecanismos de mejora continua, alineados con los objetivos estratégicos institucionales. De este modo, la seguridad de la información se concibe como un proceso dinámico, capaz de adaptarse a los cambios del entorno tecnológico, normativo y organizacional.

En este contexto, la norma ISO/IEC 27001:2022 se consolida como el referente internacional para el diseño, implementación, mantenimiento y mejora continua de un SGSI. Su relevancia radica en su carácter certificable y en su rol como norma central de la familia ISO/IEC 27000, lo que permite a las organizaciones demostrar de manera objetiva su compromiso con la seguridad de la información ante las partes interesadas internas y externas.

De acuerdo con la Organización Internacional de Normalización (2022a), los requisitos de la ISO/IEC 27001 se estructuran conforme al enfoque de gestión basado en el ciclo de mejora continua Planificar-Hacer-Verificar-Actuar (PHVA), e incluyen los siguientes componentes: contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora continua. La norma inicia con el análisis del contexto organizacional, considerando los factores internos y externos, las necesidades y expectativas de las partes interesadas y la definición del alcance del SGSI, lo que permite alinear la gestión de la seguridad de la información con los objetivos estratégicos institucionales.

Asimismo, la ISO/IEC 27001 enfatiza el rol del liderazgo de la alta dirección, a quien se atribuye la responsabilidad de establecer la política de seguridad de la información, asignar roles y responsabilidades, y asegurar la disponibilidad de los recursos necesarios para la correcta operación del sistema. La planificación se fundamenta en la gestión de los riesgos de seguridad de la información, orientando la definición de objetivos y la selección de controles adecuados para su tratamiento. De igual forma, la norma contempla los elementos de soporte, tales como la gestión de recursos, la competencia y concienciación del personal, la comunicación organizacional y el control de la información documentada.

En el ámbito operativo, la ISO/IEC 27001 establece la necesidad de implementar y controlar los procesos definidos, así como de gestionar los cambios que puedan afectar el desempeño del SGSI. Finalmente, los procesos de evaluación del desempeño y mejora continua permiten verificar la eficacia del sistema, identificar no conformidades y oportunidades de mejora, y fortalecer de manera sistemática la protección de la información en un entorno organizacional dinámico y en constante evolución.

Por otro lado, la ISO/IEC 27002:2022 complementa a la ISO/IEC 27001:2022 al proporcionar orientación detallada sobre un conjunto de controles de seguridad de la información, que sirven como referencia para que las organizaciones puedan adoptarlos a fin de proteger su información a través de políticas de seguridad y planes de contingencia o de recuperación ante desastres. La norma establece un total de 93 controles de seguridad, los cuales se organizan en cuatro categorías: organizacional, personal, físico y tecnológico. Estas categorías abarcan controles relacionados con la gobernanza, la gestión de riesgos y las políticas institucionales; la seguridad asociada a los recursos humanos y la concienciación del personal; la protección de las instalaciones y del entorno físico; y la seguridad de los sistemas de información, las redes, las aplicaciones y los activos tecnológicos que soportan los procesos organizacionales. (Organización Internacional de Normalización, 2022b; Katz, 2025).

La ISO/IEC 27003:2017 proporciona una guía práctica para la implementación de un SGSI alineado con los requisitos de la ISO/IEC 27001. Aunque su aplicación no es obligatoria para efectos de certificación, contribuye significativamente a mejorar la claridad, coherencia y flexibilidad en el diseño e implementación del sistema (Jennings, 2025a).

De manera complementaria, la ISO/IEC 27004:2016 ofrece directrices para supervisar, medir, analizar y evaluar el desempeño del SGSI. Esta norma permite a las organizaciones valorar la eficacia de sus controles de seguridad y fomenta la mejora continua de la gestión de la seguridad de la información, consolidando así un enfoque integral y sistemático en la protección de los activos de información (Jennings, 2025b).

Igualmente, la ISO/IEC 27005:2022 se enfoca en guiar a las organizaciones en la identificación y gestión de riesgos relacionados con el sistema de gestión de seguridad de la información. El propósito es ofrecer una visión general de las amenazas y vulnerabilidades específicas de los activos de información, determinar las implicaciones y la gravedad de cada escenario de riesgo dado y así definir las opciones específicas de solución para su tratamiento (Bonnie, 2023). Los activos de información son elementos, tangibles o intangibles, que tienen valor y que son susceptibles de ataques deliberados o accidentales con consecuencias que pueden tener un impacto significativo para una organización. Incluyen: datos, servicios, plataformas informáticas, equipos informáticos, soportes electrónicos, redes de comunicación, equipamiento auxiliar, recursos físicos y recursos humanos (Esquema Nacional de Seguridad, 2012).

Cabe señalar que la familia ISO/IEC 27000 incluye otras normas complementarias que abordan aspectos específicos de la seguridad de la información, tales como auditorías y privacidad de datos. No obstante, las normas ISO/IEC 27001, 27002, 27003, 27004 y 27005 son las más destacadas, por su carácter central, certificable y su utilidad práctica en la implementación, gestión y evaluación de un SGSI.

Por su parte, la norma ISO 16363:2025 proporciona un marco para la auditoría y certificación de repositorios digitales confiables, mediante la evaluación de su capacidad para preservar a largo plazo la integridad, autenticidad y accesibilidad de los documentos digitales. Esta norma abarca aspectos organizativos, tales como la gobernanza institucional y la gestión de los objetos digitales, así como elementos relacionados con la seguridad de la infraestructura, más allá de la dimensión puramente tecnológica (The Consultative Committee for Space Data Systems. 2024). No obstante, aunque la seguridad de la información forma parte de los criterios de evaluación de la ISO 16363, el abordaje sistemático y transversal de este aspecto se fundamenta principalmente en la ISO/IEC 27001, norma diseñada específicamente para la gestión integral de los procesos de seguridad de la información de una organización.

Estas normas son plenamente aplicables a instituciones como los archivos históricos. Sin embargo, la implementación de un sistema de gestión de seguridad de la información en estos servicios enfrenta un desafío enorme, considerando que, en muchos casos, los archivos históricos carecen de un presupuesto plenamente establecido, además, en la región de Latinoamérica, cuentan con personal profesional insuficiente o poco capacitado en el área. A lo mencionado se suma que los archivos suelen estar desorganizados puesto que no son concebidos como un sistema de información integral y, en algunos casos, los archivos parecen auténticos almacenes olvidados por las instituciones a las que están adscritos (Medina Morales, 2015). Esta realidad limita significativamente la capacidad de los archivos para mejorar sus servicios y proteger la memoria colectiva.

En cuanto a los estudios relacionados con este ámbito, se han encontrado algunas investigaciones. Por ejemplo, una de ellas corresponde a un diagnóstico respecto a la disponibilidad de políticas públicas archivísticas existentes en Iberoamérica, realizado por el programa Iberarchivos (Basualdo, 2023). En el referido informe se incluye una sección dedicada a la existencia de normativas de seguridad, se destaca que Argentina, España, Portugal y República Dominicana cuentan con estándares que incluyen leyes de protección de datos personales y resoluciones gubernamentales. Por su parte, Chile y Filipinas refieren a la implementación de prácticas internacionales como la ISO 27001:2013. De igual modo, Panamá y Ecuador hacen uso de sistemas de detección de intrusos y firewalls como parte de las medidas de seguridad adoptadas.

Asimismo, la investigación de Abirov *et al.* (2025) propone un método para validar la integridad, fiabilidad y accesibilidad de los archivos históricos a través de un enfoque descentralizado que aprovecha tecnologías como *blockchain*, hash criptográfico y contratos inteligentes. En este contexto, el *blockchain* se define como un registro distribuido e inmutable que almacena transacciones o eventos en bloques encadenados de forma segura, lo que permite garantizar la trazabilidad y la no alteración de la información a lo largo del tiempo. El hash criptográfico corresponde a una función matemática que transforma un conjunto de datos en un valor único de longitud fija, actuando como una huella digital del documento y permitiendo detectar cualquier modificación no autorizada. Por su parte, los contratos inteligentes son programas autoejecutables que operan sobre la red *blockchain* y que permiten automatizar reglas, validaciones y procesos previamente definidos, asegurando el cumplimiento de condiciones específicas sin la intervención de intermediarios (IBM, s. f.). En conjunto, este enfoque garantiza que los documentos se mantengan auténticos y accesibles para las generaciones futuras siendo completamente aplicable al entorno archivístico.

De manera similar, un estudio realizado por Fernal (2022) se centra en analizar el impacto del *blockchain* en el contexto de los documentos de archivos digitales en sistemas descentralizados, proponiendo un modelo lógico para la aplicación de esta tecnología en la autenticación distribuida automatizada a lo largo del ciclo de vida de los documentos digitales. En este contexto, la autenticación se entiende como el proceso mediante el cual se verifica y confirma la identidad de los usuarios, sistemas o entidades que interactúan con los documentos, garantizando que solo aquellos debidamente autorizados puedan acceder, modificar o validar la información.

Por su parte, la investigación de Rabelo (2023) tiene como objetivo principal examinar los efectos de la implementación del *blockchain* en los archivos en términos de autenticidad y autenticación, así como analizar los requisitos necesarios para la adopción de esta tecnología en entornos archivísticos.

A pesar de estos avances significativos en materia de seguridad, y de su relevancia como medidas de autenticación en los sistemas informáticos de gestión documental, no se ha encontrado bibliografía que aborde de manera integral la implementación de SGSI en los archivos latinoamericanos, incluyendo tanto el manejo de políticas

institucionales de seguridad, la gestión de recursos humanos, como la protección de la infraestructura física y tecnológica, especialmente en países de la región donde los archivos aún se encuentran en etapas iniciales de implementación. Además, no se ha comprobado que dichos archivos hayan adoptado medidas de seguridad de la información suficientes para garantizar la integridad, disponibilidad y confidencialidad de sus documentos.

Según un censo realizado por el Ministerio de Cultura de España (2024), existen 16989 archivos en Latinoamérica que resguardan fondos distribuidos en varias categorías como archivos municipales, religiosos, universitarios, históricos, sanitarios, empresariales, parroquiales, bancarios, judiciales, generales, personales, notariales, militares, monásticos, sindicatos, entre otros, lo que destaca la importancia de asegurar la protección de sus acervos. Por lo tanto, es urgente fortalecer la seguridad de los archivos para garantizar el resguardo de su patrimonio documental.

Dado el gran número de archivos existentes en la región, se tomaron en cuenta a los archivos históricos y, en vista de que no se dispone de datos de contactos actualizados de sus responsables en cada país, se utilizó como referente a los archivos generales nacionales, también denominados en algunos países como archivos nacionales, puesto que sus objetivos principales son recopilar, preservar, organizar y difundir el patrimonio documental del país. Además, desempeñan un rol normativo y de supervisión sobre la gestión documental nacional (Gobierno de México, s. f.). Por lo tanto, constituyen una base para conocer la realidad de cada país latinoamericano, transformándose así en un tema de mucho interés para conocer su situación actual en materia de seguridad de la información.

Con estos antecedentes, esta investigación tiene el propósito de diagnosticar el estado de implementación de los SGSI en los Archivos Generales Nacionales de América Latina, fundamentándose en las recomendaciones establecidas por la familia de normas ISO/IEC 27000. Los resultados permitirán conocer su situación a fin de evaluar las prácticas actuales de seguridad, identificar posibles áreas de mejora y constatar si se están tomando las medidas adecuadas para proteger tanto los activos de información físicos como digitales. La información obtenida también contribuirá al desarrollo de estrategias para fortalecer la seguridad en el manejo y almacenamiento de documentos y datos sensibles en los archivos.

Metodología

Para lograr el objetivo planteado, se aplicó una investigación con enfoque cuantitativo, incluyendo la técnica de muestreo probabilístico estratificado. La población seleccionada estuvo compuesta por archivos históricos de Latinoamérica, subdividida en estratos distribuidos por país. En este marco, se eligieron los archivos generales nacionales como representantes de cada estrato, a fin de asegurar una muestra representativa y diversa de la región. El instrumento utilizado para la recolección de datos fue una encuesta. La investigación se desarrolló en tres etapas:

En primer lugar, con el fin de diagnosticar la implementación del sistema de gestión de seguridad de la información en los archivos generales nacionales latinoamericanos, se seleccionaron 16 países de la región pertenecientes al directorio de afiliados categoría A de la Asociación Latinoamericana de Archivo (ALA)[2]. Esta entidad promueve el desarrollo integral de los archivos y de la gestión documental en América Latina, fomentando la colaboración entre instituciones y profesionales del ámbito archivístico (Asociación Latinoamericana de Archivos, 2025).

Seguidamente, se diseñó una encuesta en la plataforma Google Forms, la cual fue enviada por correo electrónico a la Secretaría Ejecutiva de ALA, con el objetivo de que fuera distribuida entre los responsables de los archivos generales nacionales de los 16 países seleccionados. En el texto del correo se explicó el propósito del instrumento, así como el contexto de la investigación. La encuesta fue enviada el 11 de junio de 2025 y se promovió en tres ocasiones adicionales, en razón de la baja tasa de respuestas. El periodo de recolección de datos concluyó el 18 de agosto de 2025.

La encuesta constó de 25 preguntas, tanto de selección múltiple como abiertas, agrupadas en cinco segmentos temáticos:

- Datos generales del archivo: Contenía 4 preguntas orientadas a conocer datos del director del archivo, el país al que pertenece, la institución a la que está adscrito el archivo y su dirección electrónica.
- Activos de información del archivo: Incluía 5 preguntas destinadas a recopilar información sobre los tipos de activos, sus formatos y las medidas de seguridad implementadas para su protección.
- Políticas de seguridad: Compuesta por 2 preguntas relacionadas con la existencia de políticas de seguridad y programas de capacitación en la materia.
- Gestión de riesgos: Integraba 4 preguntas sobre los procesos de análisis e identificación de riesgos, así como el desarrollo de planes de contingencia.
- Gestión de la seguridad de la información: Se formularon 10 preguntas referentes a la clasificación de documentos según su nivel de sensibilidad, los controles de acceso a la información, la protección de soportes electrónicos, la realización de auditorías internas, los procedimientos para la eliminación segura de la información y el conocimiento de la norma ISO 27001. Asimismo, se incluyó un espacio abierto para comentarios o sugerencias adicionales.

Finalmente, los datos obtenidos fueron tabulados en Microsoft Excel y presentados mediante tablas porcentuales, con el propósito de dar a conocer un panorama claro y detallado del estado de implementación de sistemas de gestión de seguridad de la información en los archivos generales nacionales de Latinoamérica.

2 Directorio de archivos generales de la nación afiliados en la categoría A de ALA: https://alaarchivos.org/lista-de-miembros-clase-a/.

Discusión de Resultados

La encuesta fue completada por 11 directores de archivos generales nacionales, lo que representa una tasa de respuesta de 68,75 % sobre un total de 16 encuestados previstos. Este porcentaje se calculó mediante una regla de tres simple. A continuación, se presentan los resultados obtenidos, en función de los criterios establecidos en instrumento de recolección de datos:

Datos generales del archivo

El primer segmento de la encuesta se orientó en recopilar información personal de los directores de los archivos nacionales, poniendo énfasis en el país de origen y la institución a la que está adscrito el servicio. Los 11 archivos nacionales latinoamericanos encuestados corresponden a los siguientes países: México, El Salvador, República Dominicana, Perú, Ecuador, Costa Rica, Bolivia, Puerto Rico, Panamá, Chile y Colombia.

Estos datos recopilados permiten trazar una visión general sobre la representación geográfica de los archivos nacionales en la región, lo cual es indispensable para poner en contexto los resultados obtenidos en los apartados posteriores de la encuesta.

Activos de información del archivo

En el segmento dedicado a los activos de información del archivo, se recabaron los siguientes resultados, los cuales detallan la disponibilidad de los diferentes tipos de activos, sus formatos y las medidas implementadas en materia de seguridad de la información en los archivos nacionales latinoamericanos:

Respecto a los activos de información presentes en el archivo, se recopiló la siguiente información:

Tabla 1. Cantidad de archivos nacionales que disponen de los activos de información

N.°	Activos de información	Archivos que disponen de los activos
1	Información pública	11 (100 %)
2	Computadores personales	10 (90,9 %)
3	Aplicaciones informáticas	10 (90,9 %)
4	Routers	10 (90,9 %)
5	Impresoras	9 (81,8 %)
6	CD u otros soportes electrónicos	9 (81,8 %)
7	Servidores	9 (81,8 %)
8	Escáneres o digitalizadores	8 (72,7 %)
9	Teléfonos IP	7 (63,6 %)
10	Información sensible	7 (63,6 %)

La Tabla 1 presenta la distribución de los activos de información en los archivos generales nacionales latinoamericanos. En síntesis, la mayoría de los archivos disponen de activos básicos como computadoras personales, acceso a la información pública, aplicaciones informáticas, routers, impresoras y CD u otros soportes electrónicos. Lo que indica que estos activos son recursos comunes y bastante accesibles en la mayoría de los archivos. No obstante, según los datos recopilados, los archivos muestran una infraestructura básica bien definida. Un aspecto interesante es que solo 7 archivos gestionan información sensible, este dato pone de manifiesto la necesidad de implementar o fortalecer políticas adecuadas para su manejo y protección.

En lo que se refiere a los formatos en los que está almacenada la documentación custodiada en el archivo, los resultados arrojan la siguiente información:

Tabla 2. Cantidad de formatos de activos de información disponibles en los archivos

N.°	Formatos	Disponibilidad en archivos
1	Papel	11 (100 %)
2	Cintas de audio	10 (90,9 %)
3	Videocasetes	9 (81,8 %)
4	Discos duros externos	8 (72,7 %)
5	CD	8 (72,7 %)
6	DVD	7 (66,6 %)
7	Unidades USB	6 (54,5 %)
8	Discos de acetato	4 (36,4 %)
9	Disquetes	4 (36,4 %)
10	Otros (Servidor, Almacenamiento en red NAS y SAN, Servidores NAS QNAP, Información en la nube, celuloide)	7 (66,6 %)

La Tabla 2 pone de relieve los formatos disponibles de los activos de información en los archivos generales nacionales latinoamericanos. Se observa una presencia predominante del formato papel (11 archivos), así como una alta disponibilidad de cintas de audio y videocasetes (entre 9 y 10 archivos). Esto refleja una fuerte presencia de materiales físicos tradicionales y material audiovisual histórico.

Un número considerable de documentos de archivo está disponible en discos duros externos, CD y unidades USB y DVD (entre 7 y 8 archivos), lo que indica que existe un avance hacia la modernización en los soportes. No obstante, aún disponen de formatos antiguos como los disquetes y los discos de acetato (4 archivos), esto implica que parte del acervo documental posiblemente aún no ha sido migrado a nuevas tecnologías y se conserva en medios de almacenamiento antiguos que necesitan equipos específicos para ser utilizados, de los que no se conoce si disponen.

Conviene mencionar la presencia significativa de medios de almacenamiento, tales como almacenamiento en red NAS y SAN e incluso en la nube y servidores físicos, lo que muestra una evolución en la infraestructura del archivo. Sin embargo, también se señala la disponibilidad de celuloide, lo que fortalece la idea de una colección histórica rica y variada.

Asimismo, se les consultó a los encuestados cuáles de los activos seleccionados consideran que demandan mayor protección. En sus respuestas, manifestaron la importancia de asegurar la integridad de los datos sensibles y la necesidad de brindar atención a la información almacenada en la nube, los soportes electrónicos y los documentos en soporte de papel.

En síntesis, los archivos generales nacionales latinoamericanos disponen de una alta diversidad de formatos, desde soporte de papel hasta el almacenamiento en la nube. Se observa una marcada transición hacia lo digital, aunque el proceso aún no esté completo. La coexistencia de tecnologías obsoletas y modernas evidencia la necesidad de desarrollar e implementar un plan de preservación digital, en caso de no tenerlo, que garantice la continuidad digital a largo plazo de los documentos almacenados tanto en soportes analógicos como electrónicos.

En cuanto a los mecanismos de seguridad aplicados para resguardar los activos de información en los archivos generales nacionales, los 11 archivos (100 %) participantes afirmaron que aplican este tipo de medidas. En este contexto, manifestaron que las acciones implementadas incluyen un gran abanico de mecanismos, como el establecimiento de protocolos de seguridad, el control de acceso físico a los repositorios donde se almacenan los documentos de archivo y el uso de sistemas de autenticación y permisos para el acceso a los sistemas informáticos y de almacenamiento masivo.

Asimismo, manifestaron la aplicación del Esquema Gubernamental de Seguridad de la Información, la obtención de copias de seguridad periódicas y la protección contra malware y ciberataques mediante software antivirus y firewalls. De igual modo, se incluyen medidas como la implementación de proyectos de seguridad humana y procedimientos internos institucionales, prevención de riesgos por incendios, gestión de documentos restringidos, fumigaciones constantes en depósitos de documentos, control de préstamos y verificación de la identidad de los usuarios que consultan documentos en la sala del archivo.

En consecuencia, en este primer segmento se observa que los archivos generales nacionales latinoamericanos cuentan con una extensa variedad de soportes de almacenamiento, lo que evidencia la riqueza histórica y heterogeneidad de sus tipos documentales. Esto demuestra un compromiso proactivo respecto a la implementación de mecanismos de protección que aseguren la confidencialidad, disponibilidad e integridad de la documentación. Esta realidad esboza destacados retos en términos de preservación, lo que implica la necesidad de robustecer las técnicas de conservación de los soportes y sus políticas de seguridad.

Gestión de riesgos

Sobre el segmento de gestión de riesgos, 10 archivos (90,9 %) confirmaron la identificación de los riesgos que podrían atentar contra la seguridad de sus activos de información, mientras que 1 archivo (9,1 %) no ha realizado este proceso. Esto demuestra que la mayoría de archivos generales nacionales latinoamericanos evaluados poseen un alto nivel de responsabilidad y conciencia en relación con las posibles amenazas que podrían poner en peligro la integridad de la información y han tomado medidas preventivas para enfrentar debidamente futuros riesgos potenciales.

En cuanto a la periodicidad de actualización del análisis de riesgos, de los 10 archivos que afirmaron identificar los riesgos relacionados con la seguridad de la información, se evidencia que 3 archivos (33,3 %) realizan un análisis de riesgos anual, lo cual podría no ser lo suficientemente alto para atender imprevistos. Por otra parte, 1 archivo (11,1 %) señaló que lleva a cabo el referido análisis de manera semestral, lo que demuestra una actitud comprometida frente a posibles incidentes. Los 5 archivos restantes (55,6 %) indicaron no haber determinado una frecuencia de análisis específica, lo que evidencia la falta de sistematización a la hora de evaluar riesgos, aumentando así la probabilidad de no identificar peligros y exponerse a amenazas en el entorno de seguridad del archivo.

Este análisis refleja que, aunque la gran mayoría de archivos llevan a cabo algún tipo de análisis de riesgos, la falta de frecuencias en la ejecución de los mismos plantea la urgencia de definir protocolos regulares a fin de mitigar posibles incidentes que podrían afectar negativamente a los archivos y mejorar la gestión de sus riesgos.

Sobre el desarrollo o implementación de planes de contingencias o recuperación ante desastres en el archivo, 8 participantes (72,7 %) indicaron que sí disponen de un plan de contingencia o de recuperación de desastres. Este dato evidencia que los archivos han tomado medidas enfocadas hacia la resiliencia organizacional y protección frente a incidentes inesperados que pudieran interrumpir la continuidad operativa.

No obstante, los 3 archivos restantes (27,3 %) manifestaron no contar con estos tipos de planes. La falta de planes de contingencia o de recuperación ante desastres puede poner en riesgo la integridad de la información y la capacidad operativa del archivo en situaciones de emergencia, por lo que es imperativo fortalecer los protocolos de preparación para minimizar riesgos y mejorar su capacidad de respuesta ante situaciones adversas. De los 8 directores de archivos que afirmaron disponer de un plan de contingencia o de recuperación ante desastres, los aspectos que han contemplado en los referidos documentos son:

Tabla 3. Aspectos contemplados en los planes de contingencia disponibles en los archivos

N.°	Aspectos contemplados	Disponibilidad en archivos
1	Amenazas de origen industrial (inundaciones, explosiones, suciedad, humedad, etc.)	7 (87,5 %)
2	Desastres naturales	6 (75 %)
3	Errores humanos en el uso de los documentos	6 (75 %)
4	Ataques informáticos	5 (62,5 %)

La Tabla 3 evidencia que la mayoría de archivos (87,5 %) contempla los riesgos asociados a amenazas de origen industrial, que incluyen inundaciones, explosiones, suciedad y humedad. Esto demuestra una preparación adecuada para enfrentar posibles eventos en el entorno físico. De igual modo, un 75 % también ha considerado los desastres naturales, lo que demuestra que existe una alta conciencia sobre la necesidad de proteger los activos de información ante incidentes como incendios, terremotos, inundaciones, etc.

De manera similar, el 75 % manifiesta que ha tenido en cuenta el riesgo de errores humanos en el uso de los documentos. Este aspecto es muy importante puesto que los fallos producidos por el ser humano son comunes y pueden derivar en riesgos significativos en la seguridad de la información.

Por otro lado, el 62,5 % señala que se ha contemplado el riesgo de ataques informáticos, lo que refleja una menor cobertura frente a amenazas en comparación con los riesgos de carácter físico, resaltando la necesidad de robustecer las medidas de protección de la información en los archivos generales nacionales latinoamericanos.

En conclusión, los resultados mostrados evidencian que los archivos generales nacionales de América Latina necesitan fortalecer sus medidas de seguridad en el entorno físico y digital para garantizar una protección integral de sus activos de información y su continuidad operativa. De esta manera, se logrará una cultura organizacional efectiva y robusta.

Políticas de seguridad

En el segmento dedicado a las políticas de seguridad, los resultados arrojan que 10 archivos (90,9 %) reportaron que su institución dispone de políticas establecidas, mientras que 1 archivo (10 %) carece de ellas. Estos resultados demuestran un elevado grado de cumplimiento en cuanto a la existencia de políticas de seguridad como un instrumento primordial para determinar mecanismos y controles de protección de los activos de información de los archivos frente a amenazas existentes, fomentando así el uso responsable de los activos de información.

Respecto a la formación continua recibida para implementar las políticas de seguridad, 4 archivos (36,4 %) confirmaron que han recibido capacitaciones, mientras que 4 archivos (36,4 %) manifestaron haber sido formados esporádicamente. Los 3 archivos restantes (27,3 %) indicaron nunca haber recibido ningún tipo de capacitación en la materia.

Por lo tanto, estos resultados revelan la imperiosa necesidad de garantizar la aplicación efectiva de las políticas de seguridad archivísticas. Esto depende, en gran medida, de la capacitación y sensibilización del personal involucrado tanto en el área de tecnologías como en la gestión documental. Las brechas de capacitación identificadas ponen de relieve la necesidad de establecer programas formativos proactivos, que promuevan una cultura organizacional comprometida enfocada en proteger los documentos y sus soportes, tanto en formato analógico como electrónico, así como mejorar continuamente la gestión informacional y sus procesos de seguridad.

Gestión de la seguridad de la información

En relación al segmento de gestión de la seguridad de la información, 3 archivos (27,3 %) clasifican sus documentos de acuerdo al nivel de sensibilidad o confidencialidad de una forma completa, mientras que 7 archivos (63,6 %) se encuentran en un estado de implementación parcial. Solamente 1 archivo (9,1 %) no ha implementado ningún proceso de clasificación, lo que podría constituir un alto riesgo en materia de seguridad de la información, puesto que al no diferenciar entre la información pública, reservada o crítica se complica la capacidad de priorización de acciones de recuperación, y los documentos quedan expuestos a amenazas y posibles filtraciones de información. Esto demuestra la relevancia de fortalecer las políticas de seguridad de los documentos, por cuanto la ausencia de clasificación documental, de acuerdo al nivel de sensibilidad o confidencialidad, impide aplicar niveles adecuados de protección, dejando al archivo vulnerable frente a múltiples amenazas.

Además, se consultó sobre los controles de acceso a la información implementados en el archivo. En respuesta, los directores de los archivos generales de la nación han señalado que disponen de los siguientes mecanismos de control:

Tabla 4. Controles de acceso a la información implementados en los archivos nacionales

N.°	Controles implementados	Disponibilidad en archivos
1	Acceso físico restringido al acervo	10 (91 %)
2	Gestión de contraseñas para equipos y sistemas	9 (81,8 %)
3	Registros de acceso o bitácoras	9 (81,8 %)
4	Biométricos de acceso	2 (18,2 %)
5	No existen controles de acceso	0 (0 %)

La Tabla 4 demuestra que los controles de acceso físico restringido al acervo documental tienen una alta implementación en los archivos (91 %). Esto significa que la gran mayoría están protegidos físicamente, lo que previene el acceso no autorizado, en base a lo estipulado en ISO/IEC 27002 (Organización Internacional de Normalización, 2022b), en cuanto a controles físicos. Esta práctica de seguridad es fundamental para evitar daños, robos o divulgación no autorizada de información crítica.

Asimismo, el 81,8 % de los archivos han implementado correctamente la gestión de contraseñas. Esta medida es imprescindible para proteger los sistemas informáticos frente a accesos no autorizados. Es importante garantizar que las contraseñas utilizadas sean fuertes y que haya una adecuada administración de las mismas a fin de protegerse de las vulneraciones de datos y garantizar el acceso seguro de personas autorizadas a sistemas y equipos (Microsoft, 2025).

Otro aspecto que tiene bastante aceptación es la implementación de registros de acceso o bitácoras (81,8 %). Las bitácoras son fundamentales para auditar y rastrear el acceso a los sistemas informáticos (quién, cuándo y qué acciones realiza). Gracias a esto se detectan posibles incidentes de seguridad o comportamientos sospechosos. No obstante, es muy importante asegurar que estos registros se revisen de manera regular.

Por otro lado, la implementación de biometría (reconocimiento facial, huellas dactilares, entre otros) es muy baja (18,2 %). Los sistemas biométricos son una medida avanzada para garantizar un acceso seguro. Los resultados demuestran que los archivos no están aprovechando las bondades de estas tecnologías, lo que podría significar un área de mejora, particularmente en entornos con información crítica.

En consecuencia, se evidencia que se ha realizado una implementación sólida de medidas básicas de acceso como restricción de acceso y gestión de contraseñas. No obstante, se recomienda mejorar las medidas de seguridad, especialmente en lo relativo a controles de acceso avanzados como la biometría a fin de garantizar la protección de los sistemas y la información.

Por otro lado, resulta de mucho interés conocer los mecanismos de protección de la información almacenada en soportes electrónicos. Con este fin, los directores de los archivos manifestaron que han implementado las medidas que se presentan a continuación:

Tabla 5. Medidas de protección de la información almacenada en soportes electrónicos

N.°	Controles implementados	Aplicación en archivos
1	Copias de seguridad periódicas (backups)	10 (91 %)
2	Cifrado de la información	3 (27,3 %)
3	Otros (Servidores en espejo, firewall)	2 (18,2 %)
4	No se realizan medidas de protección	0 (0 %)

La Tabla 5 muestra la implementación de diferentes controles de protección de la información en archivos, junto con su aplicación en términos porcentuales. El 91 % de los archivos han implementado copias de seguridad periódicas, lo que evidencia que una gran parte de instituciones están protegiendo su información a través de respaldos.

Solo un pequeño grupo de archivos (27,3 %) ha adoptado la encriptación de la información. Esto indica que es una medida menos común en relación con la implementación de copias de seguridad, aunque es una práctica importante para garantizar la confidencialidad de los datos. Finalmente, dos archivos (18,2 %) han implementado otros controles de seguridad como servidores en espejo o firewalls, lo que demuestra que estas soluciones adicionales de protección son menos frecuentes.

En síntesis, la gran mayoría de archivos pone énfasis en realizar copias de seguridad. No obstante, los controles más avanzados, como el cifrado y otras soluciones de seguridad, son los menos frecuentes. Conviene destacar, como elemento favorable, que no se observaron instituciones archivísticas sin protección alguna.

Sobre la formación continua en el ámbito de la seguridad que reciben los archivistas y el personal que lleva a cabo el proceso de gestión documental, 5 encuestados (45,5 %) indicaron que el personal recibe capacitación continua periódicamente, lo cual constituye un acierto puesto que permite mantener estándares apropiados de protección de información. Por otra parte, 4 (36,4 %) manifestaron que se capacitan de manera esporádica y 2 instituciones archivísticas (18,2 %) señalaron que no han recibido formación en el ámbito, lo que evidencia una brecha significativa en la concientización y la sensibilización sobre seguridad de la información.

Respecto al monitoreo o auditorías internas de la gestión de la seguridad de la información, el 54,5 % de los directores de los archivos llevan a cabo estas prácticas y desarrollan la documentación asociada, lo cual es necesario para garantizar la trazabilidad y la mejora continua. De igual modo, el 36,4 % realiza las auditorías y el monitoreo, pero no genera la documentación correspondiente, lo que dificultaría la evaluación y el seguimiento de los resultados. Para concluir, un 9,1 % indicó desconocer la ejecución de estas actividades, lo que evidencia una falta de claridad y comprensión de la relevancia del proceso de monitoreo o auditoría.

En cuanto a la disponibilidad de procedimientos de eliminación segura de los documentos, el 9,1 % de archivos dispone de mecanismos para la eliminación de la documentación exclusivamente en soporte físico, mientras que otro 9,1 % cuenta con mecanismos específicamente para documentos electrónicos. Un grupo mayor (36,4 %) ha implementado procedimientos tanto para documentos físicos como electrónicos, lo que demuestra un enfoque más completo hacia una eliminación segura de información. Finalmente, el 36,4 % de los archivos manifestaron que no han definido procedimientos para la eliminación segura de ninguno de estos tipos de documentos, lo cual es preocupante puesto que esto podría poner en riesgo la información crítica ante posibles amenazas de robo por parte de personas malintencionadas.

En relación a la familiaridad con la norma ISO/IEC 27001 sobre requisitos para implementar Sistemas de Gestión de Seguridad de la Información, el 54,5 % de archivos manifiesta que conoce e implementa esta norma en sus archivos, lo que refleja un compromiso con las mejores prácticas de gestión de seguridad de la información. No obstante, el 36,4 % afirma conocerla, pero no la aplica, lo que evidencia dificultades para aplicar sus principios en la práctica. Por último, el 9,1 % restante no aplica la norma, lo que sugiere una oportunidad para capacitar y sensibilizar a los archivos sobre su importancia y beneficios. En términos generales, aunque el conocimiento de la norma está extendido, se podría promover la implementación de sus buenas prácticas a fin de fortalecer la seguridad de la información en todas las áreas.

Asimismo, se consultó sobre la necesidad de fortalecer la seguridad de la información en el archivo. Al respecto, 9 instituciones archivísticas (81,8 %) reconocen la importancia de mejorarla. El hecho de identificar y conocer las posibles áreas de desarrollo y mejora demuestra su compromiso con su labor.

Por otra parte, 1 institución archivística (9,1 %) considera que no es necesario implementar mejoras, lo que indica una posible subestimación de los riesgos o de suficiencia en sus controles actuales. Finalmente, 1 archivo (9,1 %) manifestó desconocer si se requiere fortalecer la seguridad en su institución. En general, estos resultados destacan la importancia de fomentar una evaluación continua de los controles de seguridad y promover la capacitación continua del personal para garantizar una gestión de la seguridad de la información consciente y proactiva que afronte los desafíos en la materia.

A los directores que contestaron afirmativamente a la necesidad de fortalecer la seguridad de la información, se les solicitó que precisen los aspectos que consideran prioritarios. Con base a sus respuestas, indicaron lo siguiente:

Entre las acciones consideradas necesarias, destacan: controlar la descarga de información y documentos, mejorar los niveles de acceso a la información de acuerdo al perfil de usuario, renovar tecnológicamente las plataformas, implementar medidas más rígidas y robustecer la ciberseguridad. Asimismo, señalaron la necesidad de mantener un monitoreo constante de la seguridad de la información institucional y la que involucra a los funcionarios.

Actualmente, se encuentran en proceso de mejora continua de los protocolos en base a la experiencia institucional. Están implementando medidas administrativas, técnicas y físicas a fin de fortalecer la seguridad de la información y actualizar los sistemas de protección disponibles.

Un área crítica identificada es la capacitación de los funcionarios en general, por lo que se enfatiza la importancia de incrementar las formaciones en materia de seguridad. Además, plantean la creación de cuentas de usuarios diferenciadas: específicas para funcionarios y temporales para investigadores, con el propósito de tener un mayor

control y trazabilidad sobre las actividades en los sistemas y plataformas (como descargas, cargas, modificaciones, accesos).

Finalmente, también consideran fortalecer la cultura organizacional, promover el uso responsable de los recursos tecnológicos, mejorar los sistemas de monitoreo, implementar tecnologías complementarias de respaldo de información y fomentar la actualización constante de los controles de seguridad frente a nuevas amenazas.

En conclusión, los resultados ponen de relieve que, si bien existe un nivel significativo de concientización sobre la relevancia de gestionar la seguridad de la información, aún persisten retos destacados en su implementación efectiva. La mínima aplicación de estándares internacionales relacionados con la gestión de la seguridad de la información, como la familia de normas ISO/IEC 27000, deja en claro la urgencia del fortalecimiento institucional en este ámbito a través del monitoreo permanente, actualización tecnológica y procesos de capacitación continua.

Las brechas formativas de los archivistas y la adopción parcial de medidas administrativas, técnicas y físicas, junto con la falta de procedimientos estandarizados en algunos archivos, destaca la importancia de avanzar hacia una gestión de seguridad sistemática e integral.

En este marco, una cultura organizacional sólida enfocada en la seguridad de la información resulta primordial porque permite asegurar su disponibilidad, confidencialidad e integridad. En consecuencia, se sugiere desarrollar protocolos robustos, mecanismos de control y políticas claras adaptadas a las condiciones de los servicios de archivo, fortaleciendo una mejora continua en su gestión y garantizando una continuidad digital de la información a largo plazo.

Conclusiones y recomendaciones

El estudio realizado respecto a la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) en base a la ISO/IEC 27001 en los archivos generales nacionales de Latinoamérica presenta un panorama de avances parciales, en el que se combinan importantes áreas de mejora con prácticas positivas. La mayoría de los archivos ha integrado controles básicos de resguardo, políticas de seguridad y un compromiso inicial hacia la protección de los activos de información. No obstante, persisten brechas significativas en la aplicación de controles avanzados, la falta de plena adopción de estándares internacionales como la familia de normas ISO/IEC 27000 y la gestión de riesgos en el archivo, así como la carencia de formación continua de los archivistas, lo que compromete la confidencialidad, integridad y disponibilidad de la memoria histórica de la región.

Esta investigación pone en evidencia que la falta de formación continua de los archiveros constituye un aspecto crítico que limita la eficacia de las políticas y controles existentes. Sin una cultura organizacional consciente y preparada en materia

de seguridad de la información, la probabilidad de materialización de amenazas se incrementa, comprometiendo no solo la información custodiada en los archivos, sino también la confianza pública y la credibilidad institucional.

La simultaneidad de los soportes tanto analógicos como electrónicos, sumada a la existencia de tecnologías obsoletas, esboza la necesidad urgente de diseñar e implementar estrategias integrales de preservación digital segura y migración tecnológica. Esta situación refleja un compromiso con la continuidad digital de la información y garantiza integridad, fiabilidad y autenticidad de la memoria histórica a largo plazo. De igual modo, la ausencia de procedimientos estandarizados para la eliminación segura de información y la escasa implementación de medidas de cifrado y biometría demuestran la existencia de vulnerabilidades que podrían ser explotadas por los atacantes.

En este marco, resulta fundamental que los ministerios o instituciones de las cuales dependen los Archivos Generales Nacionales de Latinoamérica elaboren lineamientos institucionales en coordinación previa con la Dirección de Seguridad de la Información correspondiente, incorporando las recomendaciones expuestas en esta sección para la implementación de un Sistema de Gestión de la Seguridad de la Información basado en la familia de normas ISO/IEC 27000. Ello permitirá fortalecer la gestión pública, promover la transparencia, preservar el patrimonio documental y garantizar la adecuada protección de los datos, contribuyendo, entre otros aspectos, a:

- Modernizar la infraestructura tecnológica mediante la migración de información desde soportes obsoletos hacia medios más avanzados, sustentada en planes sólidos e integrales de preservación digital que aseguren la integridad y accesibilidad de los archivos a largo plazo.
- Estandarizar los protocolos de gestión de riesgos, estableciendo una periodicidad definida y sistemática para su análisis e incorporando la evaluación de diversos tipos de amenazas, incluyendo riesgos de origen natural, industrial y aquellos derivados del error humano. Para ello, puede tomarse como referencia la metodología de análisis y gestión de riesgos MAGERIT, reconocida por su enfoque integral y estructurado.
- Fortalecer la capacitación y profesionalización de los archivistas mediante programas de formación continua, con el fin de actualizar y consolidar sus conocimientos en gestión de seguridad de la información. Dichos programas deberían abordar, entre otros aspectos, la gestión de riesgos, la aplicación de normas internacionales como la ISO/IEC 27001, la preservación digital, la protección de datos personales, la ciberseguridad en entornos archivísticos, el uso de tecnologías emergentes como blockchain, así como la gestión de incidentes y la continuidad del negocio, contribuyendo a una práctica archivística más segura, resiliente y alineada con los estándares internacionales.
- Reforzar los controles de seguridad avanzados, incorporando medidas como autenticación biométrica, autenticación multifactor (MFA), encriptación de la información y revisiones periódicas de bitácoras de acceso. Asimismo,

implementar políticas estrictas para el control de copias, descargas y accesos diferenciados por perfil de usuario.

- Estandarizar procedimientos críticos para la eliminación segura de información, garantizando que los datos confidenciales y sensibles se gestionen conforme a las mejores prácticas de seguridad, normativas nacionales e internacionales, y políticas internas de la organización. Esto incluye la definición de métodos seguros de destrucción física y digital, la trazabilidad del proceso de eliminación y la asignación de responsabilidades claras, con el fin de minimizar riesgos de filtración, pérdida o uso indebido de la información.
- Adoptar de manera sistemática las mejores prácticas internacionales, en particular la familia de normas ISO/IEC 27000, acompañadas de la implementación de controles de seguridad y la ejecución periódica de auditorías internas y externas. Esta estrategia permite evaluar de manera continua la eficacia del SGSI, identificar oportunidades de mejora, garantizar el cumplimiento normativo y fomentar una cultura organizacional orientada a la mejora continua y la protección integral de la información.
- Fomentar la cooperación institucional y regional, mediante el intercambio de buenas prácticas entre archivos nacionales de Latinoamérica y organismos especializados, así como la gestión conjunta de recursos y asistencia técnica.
- La adopción de estos enfoques no solo fortalecerá la protección de la información y la preservación segura y sostenible del patrimonio documental, sino que también permitirá que los archivos generales nacionales de Latinoamérica cumplan plenamente su misión de custodiar y garantizar la disponibilidad, integridad y confidencialidad de la información.

De este modo, estas instituciones podrán consolidarse como referentes en la región y facilitar la replicabilidad de procesos estandarizados de seguridad de la información hacia el conjunto de archivos existentes en cada país. Asimismo, su implementación en el marco de políticas públicas nacionales y regionales contribuirá a asegurar que la memoria colectiva de la región se mantenga íntegra, accesible, fiable y auténtica, en beneficio tanto de las generaciones presentes como de las futuras.

Referencias

Abirov, V., Karimov, N., Abdurazakova, S., Khasanov, Z., Saitkamolov, M. y Normurodova, S. (2025). Inmutable archives: leveraging blockchain for authenticating and preserving historical texts. 2025 *International Conference on Computational Innovations and Engineering Sustainability (ICCIES)* (pp. 1-5). 10.1109/ICCIES63851.2025.11032909.

Asociación Latinoamericana de Archivos. (2025). *Objetivos*. https://alaarchivos.org/objetivos/

Basualdo, G. (2023). *Informe diagnóstico de políticas archivísticas*. Iberarchivos. https://iberarchivos.org/wp-content/uploads/2025/04/Informe_Diagnostico_de_Politicas_Archivisticas_2023_ES.pdf

Bonnie, E. (1 de noviembre de 2023). *El enfoque ISO 27005 para la gestión de riesgos de seguridad de la información: explicación de las actualizaciones de 2022.* Secureframe. https://secureframe.com/es-es/blog/iso-27005

Esquema Nacional de Seguridad. (2012). *MAGERIT – versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I – Método.* Ministerio de Hacienda y Administraciones Públicas. https://pilar.ccn-cert.cni.es/docman/documentos/1-magerit-v3-libro-i-metodo/file

Fernal, A. (2022). *Block e os impactos na arquivologia: um modelo lógico para autenticação distribuída dos documentos arquivísticos digitais* [Tesis doctoral, Universidade Estadual Paulista «Julio de Mesquita Filho»]. Repositorio UNESP. https://repositorio.unesp.br/server/api/core/bitstreams/74377cda-3386-417b-906e-d2eef0e3ce21/content

Gobierno de México. (s. f.). *¿Qué hacemos?* Archivo General de la Nación. https://www.gob.mx/agn/que-hacemos#:~:text=El%20Archivo%20General%20de%20la%20Naci%C3%B3n%20es%20el%20%C3%B3rgano%20que,el%20derecho%20a%20la%20memoria.

IBM. (s. f.). *¿Qué son los contratos inteligentes en blockchain?* https://www.ibm.com/es-es/think/topics/smart-contracts

Jennings, M. (11 de septiembre de 2025a). *ISO/IEC 27003:2017.* IO. https://es.isms.online/iso-27003/

Jennings, M. (11 de septiembre de 2025b). *ISO/IEC 27004:2016.* IO. https://es.isms.online/iso-27004/

Katz, E. (2 de enero de 2025). *Lista de controles ISO 27001:2022: Todo lo que necesita saber.* Spectral. https://spectralops.io/blog/iso-270012022-controls-list-everything-you-need-to-know/

Medina Morales, A. (2015). El archivo: de «almacén» a elemento de dinamización cultural. *Boletín ANABAD*, 3, 1-10. https://www.anabad.org/wp-content/uploads/2016/01/2015.3.1.pdf

Microsoft. (2025). *¿Qué es la protección con contraseña?* https://www.microsoft.com/es-es/security/business/security-101/what-is-password-protection

Ministerio de Cultura de España. (2024). *Censo- Guía de Archivos de España y de Iberoamérica.* http://censoarchivos.mcu.es/CensoGuia/directorioarchivos.htm

Organización Internacional de Normalización. (2022a). *Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de Seguridad de la Información. Requerimientos.* (Norma ISO N° 27001:2022). https://www.iso.org/es/norma/27001

Organización Internacional de Normalización (2022b). *Seguridad de la Información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. (Norma ISO N° 27002:2022)*. https://www.iso.org/es/contents/data/standard/07/56/75652.html

Rabelo, N. B. (2023). *Uso de Blockchain nos arquivos: da autenticidade à autenticação de documentos* [Tesis de maestría, Universidade Federal Fluminense]. Repositorio RIUFF. https://app.uff.br/riuff/handle/1/28912

The Consultative Committee for Space Data Systems. (2024). *Audit and Certification of Trustworthy Digital Repository.* CCSDS Secretariat. https://ccsds.org/Pubs/652x0m2.pdf

Anexo
Encuesta para la recolección de datos

Diagnóstico de implementación de sistemas de gestión de seguridad de la información en los archivos históricos nacionales de Latinoamérica

El objetivo de esta encuesta es recopilar información detallada sobre la implementación de sistemas de gestión de seguridad de la información en el archivo que usted dirige. Los datos proporcionados permitirán evaluar las prácticas actuales de seguridad, identificar posibles áreas de mejora y asegurar que se están tomando las medidas adecuadas para proteger tanto los activos de información físicos como digitales. La información obtenida también contribuirá al desarrollo de estrategias para fortalecer la seguridad en el manejo y almacenamiento de documentos y datos sensibles en los archivos.

Garantizamos que la información recopilada será tratada de manera confidencial y será utilizada exclusivamente para fines relacionados con esta encuesta.
No se recopilarán datos personales sensibles que no sean necesarios para el propósito de la misma.

Cordialmente,

María José Bravo

* Indica que la pregunta es obligatoria

Datos personales

1. **País al que pertenece:** *

2. **Nombre de la institución a la que pertenece el archivo:** *

3. **Nombre del responsable del archivo:** *

4. **Dirección de correo electrónico:** *

_____

Activos de información del archivo

5. **1. ¿Cuáles de los siguientes activos de información están presentes en su archivo?** *

(Marque todas las opciones que correspondan)

Selecciona todos los que correspondan.

- [ ] Información pública
- [ ] Información sensible
- [ ] Aplicaciones informáticas
- [ ] Impresoras
- [ ] Escáneres o digitalizadores
- [ ] Computadoras personales
- [ ] Servidores
- [ ] Teléfonos IP
- [ ] Routers u otros dispositivos de red
- [ ] CD u otros soportes electrónicos
- [ ] Otro: _____

6. **2. ¿En qué formatos está almacenada la documentación que custodia?** *

(Marque todas las opciones que correspondan)

Selecciona todos los que correspondan.

- [ ] Papel
- [ ] Discos de acetato
- [ ] Cintas de audio
- [ ] Videocasetes
- [ ] Discos duros externos
- [ ] Disquetes
- [ ] Unidades USB
- [ ] CD
- [ ] DVD
- [ ] Otro: _____

7. **3. De los activos seleccionados anteriormente, ¿Cuáles considera que requieren mayor protección?** *

8. **4. ¿Se han implementado medidas de seguridad para proteger los activos de información en su archivo?** *

   Marca solo un óvalo.

   - Si
   - No
   - Desconozco

9. **Si la respuesta a la pregunta anterior fue afirmativa, especifique en términos generales cuáles medidas de seguridad ha implementado en su archivo:**

Políticas de seguridad

10. **5. ¿Su institución cuenta con políticas de seguridad de la información?** *

    Marca solo un óvalo.

    - Si
    - No
    - Desconozco

11. **6. ¿Ha recibido capacitación en seguridad de la información?** *

Marca solo un óvalo.

- Siempre
- A veces
- Nunca

Gestión de riesgos

12. **7. ¿Se han identificado los riesgos que podrían afectar la seguridad de la información en su archivo?** *

Marca solo un óvalo.

- Si
- No
- Desconozco

13. **Si la respuesta a la pregunta anterior fue afirmativa, ¿cada cuánto tiempo se actualiza el análisis de riesgos?**

Marca solo un óvalo.

- Anualmente
- Semestralmente
- Cuando ocurre un incidente
- No hay una frecuencia establecida

14. **8. ¿Se ha desarrollado o implementado un plan de contingencia o recuperación ante desastres en su archivo?** *

Marca solo un óvalo.

- Si
- No
- Desconozco

15. **Si la respuesta a la pregunta anterior fue afirmativa, ¿Qué aspectos contempla su plan de contingencia?**

Selecciona todos los que correspondan.

- [ ] Desastres naturales
- [ ] Amenazas de origen industrial (inundaciones, explosiones, suciedad, humedad, etc.)
- [ ] Errores humanos en el uso de los documentos
- [ ] Ataques informáticos
- [ ] Otro: _____

Gestión de la seguridad de la información

16. **9. ¿Se encuentran clasificados los documentos según su nivel de sensibilidad o confidencialidad?** *

Marca solo un óvalo.

- ◯ Si, completamente
- ◯ Parcialmente
- ◯ No
- ◯ No sé

17. **10. ¿Existen controles de acceso a la información almacenada en su archivo?** *

(Marque todas las que correspondan)

Selecciona todos los que correspondan.

- [ ] Acceso físico restringido al archivo
- [ ] Gestión de contraseñas para equipos o sistemas
- [ ] Registros de acceso o bitácoras
- [ ] No existen controles de acceso
- [ ] Otro: _____

18. **11. ¿Cómo protege la información almacenada en soportes electrónicos?** *

(Marque todas las que correspondan)

Selecciona todos los que correspondan.

- [ ] Copias de seguridad periódicas (backups)
- [ ] Cifrado de la información
- [ ] No se realizan medidas de protección
- [ ] Otro: _____

19. **12. ¿El personal que maneja la documentación recibe formación específica en seguridad de la información?** *

Marca solo un óvalo.

- ◯ Sí, de forma regular
- ◯ Sí, pero esporádicamente
- ◯ No
- ◯ Desconozco

20. **13. ¿Se realiza monitoreo o auditorías internas sobre la gestión de la seguridad de la información?** *

Marca solo un óvalo.

- ◯ Sí, con la respectiva documentación
- ◯ Sí, pero no se documentan
- ◯ No
- ◯ Desconozco

21. **14. ¿Cuenta su archivo con procedimientos para la eliminación segura de la información?** *

Marca solo un óvalo.

- Sí, solo para documentos físicos
- Sí, solo para documentos electrónicos
- Sí, para documentos físicos y electrónicos
- No
- Desconozco

22. **15. ¿Conoce la norma ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información)?** *

Marca solo un óvalo.

- Sí, la aplicamos en nuestra institución
- Sí, la conozco pero no se aplica
- No

23. **16. ¿Considera que su archivo necesita fortalecer la seguridad de la información?** *

Marca solo un óvalo.

- Sí
- No
- Desconozco

24. **Si la respuesta a la pregunta anterior fue afirmativa, indique en qué aspectos considera que debería fortalecerse:**

Comentarios y sugerencias

25. **¿Desea añadir algún comentario o sugerencia adicional sobre la seguridad de la información en su archivo?**