

INFORMACIÓN Y DATOS EN TIEMPOS DE POSPANDEMIA.

Investigación, docencia y práctica profesional

Vol. 1

Georgina Araceli Torres Vargas

COORDINADORA



Z716.42

I546

Información y datos en tiempos de pospandemia : investigación, docencia y práctica profesional / coordinadora Georgina Araceli Torres Vargas. – Primera edición. – Ciudad de México : Universidad Nacional Autónoma de México, Instituto de Investigaciones Bibliotecológicas y de la Información, 2025.

2 v. – (Tecnologías de la información)

ISBN: 978-607-587-400-5 (Obra completa libro electrónico)

ISBN: 978-607-587-401-2 (v. 1 libro electrónico)

ISBN: 978-607-587-402-9 (v. 2 libro electrónico)

Bibliotecas y salud pública. 2. Pandemia de COVID-19, 2020-2023 – Aspectos sociales – Iberoamérica. 3. Bibliotecas – Innovaciones tecnológicas. I. serie. II. Torres Vargas, Georgina Araceli, coordinadora.

Diseño de cubierta: Mario Ocampo Chávez

Primera edición: junio de 2025

D.R. © UNIVERSIDAD NACIONAL

AUTÓNOMA DE MÉXICO

Instituto de Investigaciones Bibliotecológicas
y de la Información

Circuito Interior s/n, Torre II de Humanidades,
pisos 11, 12 y 13, Ciudad Universitaria, C. P.
04510, Alcaldía Coyoacán, Ciudad de México

ISBN (obra completa libro electrónico): 978-607-587-400-5

ISBN (volumen 1 libro electrónico): 978-607-587-401-2

Esta edición y sus características son propiedad
de la Universidad Nacional Autónoma de
México. Prohibida la reproducción total o
parcial por cualquier medio sin la autorización
escrita del titular de los derechos patrimoniales.

Publicación dictaminada

Hecho en México

Contenido

PRESENTACIÓN	vii
--------------------	-----

CONTEXTO TECNOLÓGICO POSPANDEMIA EN EL CAMPO DE LA INFORMACIÓN Y LA DOCUMENTACIÓN

LOS SERVICIOS DE INFORMACIÓN DIGITALES EN TIEMPOS DE POSPANDEMIA	3
Georgina Araceli Torres Vargas	

TENDENCIAS POSPANDEMIA EN EL ACCESO Y UTILIZACIÓN DE INFORMACIÓN DIGITAL PARA LA ACCIÓN CIUDADANA	15
Héctor Alejandro Ramos Chávez	

ARCHIVADO WEB EN TIEMPOS DE POSPANDEMIA. APRENDIZAJES PARA EL TRATAMIENTO DOCUMENTAL HIPERMEDIA	29
Perla Olivia Rodríguez Reséndiz	

SISTEMAS DE INFORMACIÓN Y CIBERSEGURIDAD: UN ENFOQUE DESDE LA GESTIÓN DOCUMENTAL	45
Luis Roberto Rivera Aguilera	
Julio César Rivera Aguilera	
Guadalupe Patricia Ramos Fandiño	

VANGUARDIA CIENTÍFICA Y TECNOLÓGICA EN EL CAMPO DE LA INFORMACIÓN Y LA DOCUMENTACIÓN	75
Catalina Naumis Peña	

INTELIGENCIA ARTIFICIAL Y DATOS

EL MANEJO DE DATOS Y SU APLICACIÓN EN EL CONTEXTO DE LA INTELIGENCIA ARTIFICIAL	93
Eder Ávila Barrientos	

APLICACIÓN DE LA INTELIGENCIA ARTIFICIAL GENERATIVA (IAG) EN LA ENSEÑANZA DE LA HISTORIA DE LAS BIBLIOTECAS: EXPERIENCIA PRÁCTICA	105
Miguel Ángel Gonzalo Rozas	

PANDEMIA Y POSPANDEMIA, LAS PAREDES COMO LIENZOS: UNA REVISIÓN DESDE LOS DATOS ESTRUCTURADOS	123
Ariel Alejandro Rodríguez García	
Berenice Baeza Escobedo	

SITUACIÓN ACTUAL DE LA INTELIGENCIA ARTIFICIAL EN BIBLIOTECAS	143
Juan-José Prieto-Gutiérrez	

PATRIMONIO Y TECNOLOGÍAS DIGITALES

¡YO TAMBIÉN FUI JOVEN!	163
Rosa María Fernández de Zamora	

LO EFÍMERO DE LAS COLECCIONES PERSONALES. BIBLIOTECAS NACIONALES COMO GARANTÍA DE CONSERVACIÓN Y FUTURO: EL CASO DE LA BNE Y DE LA BNM	203
Juan Carlos Marcos Recio	
Juan Miguel Sánchez Vigil	
María Olivera Zaldúa	

Sistemas de información y ciberseguridad: un enfoque desde la gestión documental

LUIS ROBERTO RIVERA AGUILERA
JULIO CÉSAR RIVERA AGUILERA
GUADALUPE PATRICIA RAMOS FANDIÑO
Universidad Autónoma de San Luis Potosí, México

INTRODUCCIÓN

En la actualidad, con la incorporación de una amplia gama de herramientas tecnológicas de ofimática y burótica en el contexto de las instituciones y organizaciones, se han diversificado las formas en las que se produce, gestiona y almacena la información. Se hace uso de distintos métodos, técnicas, procedimientos y herramientas para mantener organizada y accesible la información; en muchos de los casos, representan esfuerzos aislados que se crean en cada contexto con base en sus necesidades.

Es preciso señalar que existen varias disciplinas de la ciencia enfocadas a lograr una adecuada administración de la información que se genera en los distintos contextos sociales; éstas han sido agrupadas en las llamadas ciencias de la información, que incluyen especialidades como la gestión de información, gestión documental y archivística, documentación, museología, bibliografía, entre otras, que tienen como objetivo la gestión de información a través del tratamiento, organización, conservación, preservación y difusión.

En el presente escrito se aborda lo referente al tratamiento de información en el ámbito de la gestión documental y los archivos,

a través del diseño, desarrollo e implementación de sistemas de información, que permitan integrar estrategias y acciones de ciberseguridad con miras a mantener íntegra y segura la información digital que se genera hoy en día en las instituciones públicas y privadas.

GESTIÓN DE DOCUMENTOS

ISO 15489 – Generalidades

Toda organización que pretenda lograr resultados favorables con el manejo de su documentación invariablemente habrá de definir, como parte de sus procesos, un manual de organización que considere, a su vez, las políticas y procedimientos para dar cumplimiento a los preceptos marcados para la cadena documental en una organización.

El rol que desempeña la gestión documental en áreas administrativas, dentro de una organización, influye directamente en el cumplimiento satisfactorio de las funciones y responsabilidades que allí se desarrollan; por lo tanto, el archivo es el espacio administrativo relevante para la gestión institucional.¹

Un punto de partida imprescindible que contribuye significativamente para alcanzar el éxito será, sin duda, la implementación de estándares como la Norma ISO 15489, bajo el título general de *Información y documentación. Gestión de documentos de archivos*. Está compuesta por dos partes: la parte 1 se refiere a las generalidades; la parte 2 presenta las directrices mediante un informe técnico.

La normalización de las políticas y los procedimientos para la gestión de documentos de archivo asegura la adecuada atención y protección de éstos y, a su vez, permite que la información que

1 I. E. Zambrano, “Gestión documental en universidades”, 112.

contiene como evidencia pueda ser recuperada de manera eficiente, gracias a las prácticas estandarizadas.²

Las generalidades de la norma hacen referencia a un conjunto de acciones para la gestión de documentos en cualquier tipo de soporte, tanto de organizaciones públicas como privadas, y promueve los siguientes procesos: a) Determinación de documentos a incorporar. b) Plazos de conservación. c) Incorporación de documentos. d) Registro. e) Clasificación. f) Trazabilidad. g) Almacenamiento. h) Acceso. i) Disposición.

La conformación de una política en materia de gestión documental clara y objetiva puede derivar en múltiples beneficios en la creación, captura, almacenamiento, uso y disposición de los documentos de archivo.³

En síntesis, la Norma ISO 15489 describe una serie de conceptos y principios relativos a la gestión de documentos, los sistemas de gestión, el análisis recurrente del contexto de la organización y la identificación de los requisitos. Muestra también las políticas y responsabilidades de los involucrados en el proceso de preservación digital.⁴

Por la naturaleza y alcance del presente estudio, nos referiremos a continuación a tres procesos clave que se desprenden del tema central: almacenamiento, acceso y disposición.

a) Almacenamiento

El proceso de almacenamiento, como parte de la gestión documental, permite resguardar, gestionar y proteger la documentación. Los documentos de archivo se deberían almacenar en soportes y formatos que garanticen su disponibilidad, fiabilidad, autenticidad y conservación durante el periodo de tiempo que sea necesario.

2 Centro de Información y Documentación Científica, "Proyecto UNE-ISO 15489/1", 94.

3 A. Díaz, "Componentes para la conformación de políticas de gestión documental para universidades", 83.

4 E. M. Boderó, "Preservación digital a largo plazo", 9.

En este sentido, las organizaciones deberían seguir directrices que permitan la conservación o la migración de los documentos de archivo de un sistema de gestión a otro. Para lograrlo, necesitarían utilizar herramientas tecnológicas, protocolos de seguridad y protección de archivos digitales en diversos formatos, para garantizar su salvaguarda a lo largo del tiempo, es decir, definir políticas encaminadas a la preservación digital. Conocer con claridad los plazos de conservación de los documentos de archivo influirá en las decisiones a tomar sobre los soportes de almacenamiento.⁵

Partiendo de lo anterior, es importante señalar que los sistemas de información para la gestión de documentos de archivo habrán de considerar la disponibilidad de suficiente espacio de almacenamiento, tanto físico, a través de discos duros, como virtual, mediante servicios de hospedaje de recursos en la nube, a fin de garantizar la accesibilidad a la documentación institucional como fuente de información imprescindible para la toma de decisiones.

b) Acceso

Los permisos de acceso que se otorguen a los usuarios del sistema de gestión documental dependerán en todo momento de las condiciones legales que se establezcan, para lo cual, es de suma importancia considerar los criterios para clasificar la información y determinar si se trata de documentos con contenido de carácter público, reservado o confidencial.

Los permisos de usuario para acceso a los documentos de archivo se asignan a partir del perfil y rol de cada uno dentro del sistema de gestión documental, y permiten realizar acciones como creación, consulta, modificación o eliminación de registros o documentos. En este sentido, las organizaciones deberían disponer de directrices formales que permitieran regular a quién se les autoriza el acceso a los documentos de archivo y bajo qué circunstancias.⁶

5 CINDOC, "Proyecto UNE-ISO 15489/1".

6 CINDOC, "Proyecto UNE-ISO 15489/1".

Por otro lado, el control de acceso y su respectivo cotejo con las responsabilidades de cada usuario vinculadas a sus funciones, es un proceso constante en todos los sistemas de gestión de documentos de archivo, independientemente del formato.

En suma, la autorización para acceder a la documentación de una organización a través de un sistema de gestión documental representa una acción clave que debería ser atendida de manera colegiada y por un grupo de colaboradores interdisciplinario, de manera tal que no se ponga en riesgo la información que posee dicho sistema, y se logre así prevenir posibles conflictos de interés entre los involucrados.

c) Disposición

Las normas que regulan la disposición de documentos de archivo en los sistemas de gestión deberían aplicarse de manera sistemática y habitual. Ninguna acción de disposición debería figurar, si no se garantiza plenamente que el documento de archivo ya no será necesario, que no hay actividad pendiente de ejecución y que no existe litigio alguno o investigación que implique la utilización de dicho documento como evidencia.⁷

El proceso de disposición de documentos de archivo puede englobar:

- Destrucción física inmediata, incluyendo borrado o sobreescritura.
- Conservación durante un periodo mayor en la organización.
- Traslado a un depósito o medio de almacenamiento apropiado en control de la organización.
- Transferencia a otra entidad que haya asumido la responsabilidad.
- Traslado a un depósito gestionado por un proveedor externo.
- Transferencia de la responsabilidad de la gestión a una autoridad adecuada.

7 CINDOC, "Proyecto UNE-ISO".

Información y datos...

- Transferencia a un archivo histórico.
- Transferencia a una autoridad archivística externa.

Al diseñar e implementar un sistema de información para la gestión documental, se deberá tener presente, entre las diversas funciones y utilidades, que dicho sistema cuente con la programación y configuración que permita la elaboración del catálogo de disposición documental en sus cuatro etapas: identificación, valoración, regulación y control, para de esta manera dar el seguimiento oportuno a toda su documentación, así como a la generación de reportes en formato digital o impreso.

DISEÑO DE SISTEMAS DE INFORMACIÓN PARA GESTIÓN DOCUMENTAL

Como ya hemos señalado, la Norma ISO 15489: Información y documentación. Gestión de documentos, es un estándar creado por ISO (Organización Internacional de Normalización), y está compuesta por dos partes con las siguientes particularidades:

Proyecto UNE-ISO 15489. Parte 1: Generalidades. Campo de aplicación: regula la gestión de documentos de las organizaciones que los han producido, ya sean públicas o privadas, para clientes externos e internos.

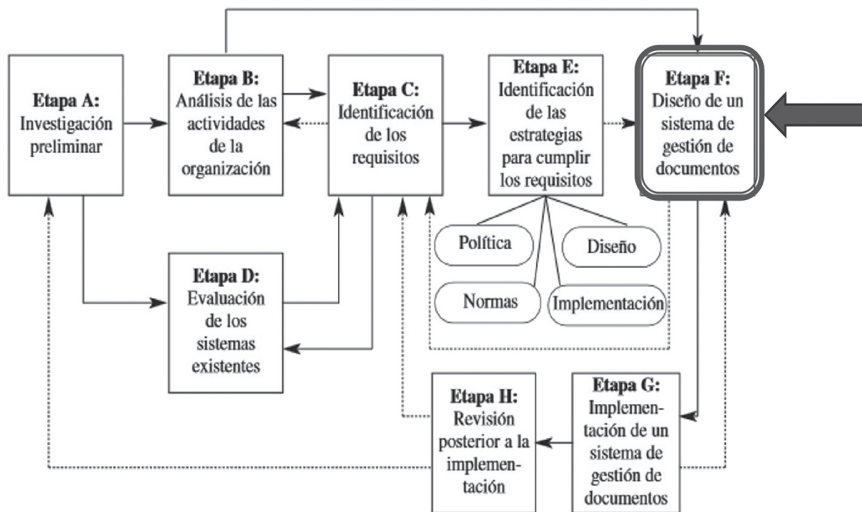
Informe técnico ISO/TR 15489. Parte 2: Directrices. Campo de aplicación: es una guía de implementación de la Norma ISO 15489 para su uso por parte de los profesionales de la gestión de documentos y de aquellas personas encargadas de gestionar documentos en sus respectivas organizaciones.

Por la naturaleza de la presente investigación, nos detendremos brevemente en la parte 2 de la ISO 15489, referente al informe técnico, Parte 2: Directrices, 3.2. Diseño e implementación de un sistema de gestión de documentos. Las etapas que lo conforman son las siguientes:⁸

8 CSIC, CINDOC, ISO/TR 15489-2.

A: Investigación preliminar, B: Análisis de las actividades de la organización, C: Identificación de los requisitos, D: Evaluación de los sistemas existentes, E: Identificación de las estrategias para cumplir los requisitos, F: Diseño de un sistema de gestión de documentos, G: Implementación de un sistema de gestión de documentos, y H: Revisión posterior a la implementación.

Figura 1. Diseño de un sistema de gestión de documentos



Fuente: Informe técnico ISO/TR 15489-1.

Diseño de un sistema de gestión de documentos (Etapa F)

El diseño de un sistema de gestión de documentos es de interés en la presente investigación, ya que proporciona los elementos técnicos a considerar en este tipo de herramientas. Según la norma y por experiencia previa, las actividades relacionadas al diseño, desarrollo e implementación de sistemas de información representan una tarea multidisciplinaria, en la que intervienen especialistas en las áreas de gestión de documentos, informática,

programación y diseño gráfico, quienes elaboran las especificaciones metodológicas, técnicas y de diseño del sistema, tomando en cuenta en todo momento las necesidades del contexto en el que se implementará la aplicación.

El informe técnico 15489-1. Parte 2: Directrices, menciona una serie de productos a crearse en el área F; de manera específica, se considera de suma importancia poner atención en los siguientes aspectos: diseño conceptual, diagramas en los que se representan la arquitectura y los componentes del sistema, especificaciones técnicas y modelo en el que se representan los elementos del sistema.

Diseño conceptual

El diseño conceptual de un sistema de información considera componentes esenciales que permiten su óptimo funcionamiento, algunos de ellos son las bases de datos, las transacciones, informes, procesos, procedimientos administrativos y usuarios; el diseño conceptual se compone de dos fases: lógico y físico, los cuales se contextualizan a continuación.

Diseño lógico: Hace referencia a lo que hará el sistema de información. Para definir los componentes, se pueden tomar en cuenta las categorías: personas, procesos, objetos y sucesos. En el caso de los sistemas para la gestión documental, es necesario que, en este apartado, se definan de inicio las tipologías documentales que existen en la organización en la que se implementará el sistema de información; cada una de estas tipologías representan las entradas de información del sistema, se pueden también proponer las áreas de la organización, los servicios o actividades que se desarrollan y las formas en que se obtendrá la información que se genera, por ejemplo, informes, reportes, estadísticas, etcétera. En el caso de los sistemas de información para el ámbito archivístico, algunos de los reportes que se pueden generar son: cuadro general de clasificación, catálogo de disposición documental, guía simple, inventarios documentales, calendario de transferencias, índices, estadísticas de usuarios, préstamos, reportes de trazabilidad, total de documentos en sistema, documentos por sección, serie, entre otros.

Como ejemplo del diseño lógico en cuanto a tipología documental se refiere, se tomará el expediente como base para contextualizar este diseño. En la identificación de este tipo de documentos, se deberán tomar en cuenta los elementos que lo conforman con base en la normativa que regula su descripción, en este caso, la norma ISAD-G.

Diseño físico: Es la forma en que se lograrán las tareas del sistema. Aquí es donde se diseña la estructura de las bases de datos del sistema a desarrollar. El diseño físico es el que permite convertir la propuesta lógica a los componentes de la base de datos; por ejemplo, si se parte del uso del modelo relacional, permite convertir las entidades en tablas, los registros en filas y las columnas en atributos. Algunos aspectos importantes por considerar en este sentido son cómo convertir entidades en tablas físicas, saber qué atributos utilizar para las columnas de las tablas físicas, qué columnas de las tablas deben definirse como claves, qué índices deben definirse en las tablas, qué vistas deben definirse en las tablas, cómo desnormalizar las tablas y cómo resolver relaciones de varios con varios.⁹

En el diseño físico de un sistema para gestión documental, se deben considerar entidades que permitan la correcta gestión de los procesos que se desarrollan en las organizaciones, con relación a la administración de información. De acuerdo con lo descrito en el apartado de diseño lógico, algunas entidades que se pueden considerar en el sistema son: usuarios, categorizándolos por súper administrador, administrador, supervisor, analista, capturista, consulta, etcétera. En cuanto a la tipología documental, se deben identificar los tipos de documentos que se generan en la organización, así como determinar sus puntos de acceso de acuerdo con la normativa, y con base en ello, crear las entidades que permitan su gestión, por ejemplo, para el documento expediente, sus atributos pueden ser: título, plazos de conservación, asunto,

9 IBM, "Diseño físico de la base de datos".

Información y datos...

código de clasificación, área, nombre del titular, valores documentales, formato, soporte, fechas extremas, total de fojas, etcétera.

Diagrama de la arquitectura del sistema de información

En lo que corresponde a la arquitectura del sistema de información, se presenta en la figura 2 un ejemplo de diagrama entidad-relación, en el que se plasma el diseño del sistema mostrando las entidades que lo conforman y las relaciones que existen entre ellas.

Aplicaciones tecnológicas. Servidor LAMP

Para llevar a cabo las etapas de desarrollo e implementación del sistema de información y con el objetivo de disminuir costos y dar viabilidad al proyecto, se recomienda considerar aplicaciones como un servidor LAMP. Estas herramientas pueden ayudar a que el proyecto de creación del sistema de información para la gestión documental no represente un impedimento para que las organizaciones no atiendan este requerimiento por falta de presupuesto. Los programas que integran esta alternativa de solución se describen a continuación.

Figura 3. Aplicaciones de servidor LAMP



Fuente: Dungeon of Bits, 2019. <https://dungeonofbits.com/instalacion-de-lampapache-mysql-o-mariadb-y-php-sobre-linux.html>.

La primera herramienta del servidor LAMP corresponde al sistema operativo Linux,¹⁰ aplicación de desarrollo libre y gratuito, lo que permite que su código fuente (abierto) se pueda utilizar, modificar y distribuir sin restricciones; forma parte de la Fundación *Software* Libre y del proyecto GNU, encargados de diseñar y distribuir la licencia pública que permitió su difusión libre. Uso: *software* de sistema que permite ejecutar diversas tareas, desde herramientas básicas de escritorio hasta lenguajes de programación y *software* de aplicación.

La segunda herramienta es el servidor HTTP Apache,¹¹ *software* destinado a crear e implementar código fuente sólido, de calidad y con muchas funciones de libre acceso (web). El proyecto es gestionado conjuntamente por un grupo de voluntarios ubicados en todo el mundo, que utilizan internet y la web para comunicar, planificar y desarrollar el servidor y su documentación relacionada. Uso: su función principal es establecer una conexión entre el

10 Jesús Santaella, “Sistema operativo Linux. ¿Cuáles son sus principales ventajas y desventajas?”.

11 Apache HTTP Server Project, “What is the Apache HTTP Server Project?”.

servidor y los distintos navegadores de internet con los usuarios del sitio web.

MySQL¹² es la siguiente aplicación del servidor LAMP. Es un sistema gestor de bases de datos relacionales para entornos web. Fue desarrollado bajo licencia dual: Licencia Pública General/Licencia Comercial por Oracle Corporation. Uso: Crea y gestiona bases de datos relacionales, algunas aplicaciones como Facebook, X (antes Twitter), Yahoo y Amazon lo utilizan.

PHP¹³ es la última aplicación que conforma el servidor. Es un lenguaje de programación de código abierto y adecuado para el desarrollo web, ya que puede ser incrustado en HTML. Uso: Su principal función es el desarrollo del *backend*¹⁴ de una web, también considera algunas acciones de *frontend*.¹⁵

Seguridad en los sistemas de información

Un aspecto importante por considerar en los sistemas de información es lo referente a la seguridad, y uno de los primeros elementos por mencionar son los usuarios que acceden a ellos; en este sentido, es conveniente mencionar que pueden existir varias categorías, entre las cuales se encuentran: administrador, supervisor, captura, consulta. A continuación, se enlistan algunas de las funciones de cada categoría.

Administrador: Crear, editar, leer, reemplazar, eliminar y cambiar posición de expediente y nivel de usuario; *Supervisor*: Copiar, renombrar, convertir, cambiar formato de archivos y documentos; *Captura*: Transformar, construir, integrar productos o formas

12 MySQL, <https://www.mysql.com/>.

13 PHP, <https://www.php.net/manual/es/intro-what-is.php>.

14 *Backend*: Acciones del desarrollo web que se encargan de los procesos necesarios para que la web se ejecute de forma correcta.

15 *Frontend*: Es la parte del software que interactúa con los usuarios, y se encarga de la conversión de datos en una interfaz gráfica para que el usuario interactúe con la información.

de presentar la información, distribuir, control total, y *Consulta*: Buscar y consultar expedientes y documentos.

Otro aspecto importante por considerar en la seguridad de los sistemas de información es lo que establece la Norma ISO 27001, la cual refiere que la seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la misma y de los sistemas implicados en su tratamiento dentro de una organización. Estos aspectos se deben cuidar en los sistemas de información para la gestión documental, ya que se trata de herramientas que coadyuvan a la gestión de la información que se genera en las instituciones tanto públicas como privadas, y para lograrlo es recomendable entender a lo que se refiere cada uno de estos conceptos. La disponibilidad considera proteger al sistema contra determinados problemas, como los intentos deliberados o accidentales de realizar un borrado no autorizado de datos, de causar cualquier tipo de denegación del servicio o de acceso a los datos, y contra los intentos de utilizar el sistema o los datos con propósitos no autorizados.¹⁶ Con relación a la integridad, se enfoca en modificaciones no autorizadas de la información, asegura la fidelidad de los datos para que sean auténticos, exactos y completos;¹⁷ con respecto a la confidencialidad,¹⁸ es preciso definir el carácter público, restringido o confidencial de la información y de los datos; en función de dicho carácter se determinará en qué lugar o soporte se puede almacenar y quiénes pueden acceder.

Con base en lo anterior, es importante mencionar la Norma ISO 27032, que define la ciberseguridad como la preservación de la confidencialidad, integridad, y disponibilidad de la información

16 Javier Aretio, *Seguridad de la información: redes, informática y sistemas de información*, 3-4.

17 Luis Joyanes, *Sistemas de información en la empresa: el impacto de la nube, la movilidad y los medios sociales*, 490-491.

18 Sixto J. Arjonilla y José A. Medina, "La gestión de los sistemas de información en la empresa: teoría y casos prácticos", 364-365.

en el ciberespacio, y lo refiere como el entorno complejo resultante de la interacción de personas, *software* y servicios de internet, a través de dispositivos tecnológicos y redes conectadas a ellas.¹⁹

CIBERSEGURIDAD

Generalidades

La ciberseguridad, de acuerdo con el portal de la compañía especializada en seguridad informática Kaspersky,²⁰ es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. Se conoce también como seguridad de tecnología de la información o seguridad de la información electrónica.

En el mismo portal de la compañía, en su capítulo para Latinoamérica,²¹ se hace mención de que el término se aplica en diferentes contextos, desde los negocios, hasta la información móvil y puede dividirse en categorías comunes, por ejemplo:

Seguridad de red. Es la práctica que consiste proteger una red informática de los intrusos, éstos pueden ser atacantes dirigidos o *malware*²² oportunista.

Seguridad de las aplicaciones. Se enfoca en mantener el *software* y los dispositivos libres de amenazas.

19 ISO, "Norma ISO 27032", <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27032:ed-2:v1:en>.

20 Kaspersky, "¿Qué es la ciberseguridad?".

21 Para conocer las noticias de ciberseguridad más recientes, se recomienda visitar su portal web, disponible en: <https://latam.kaspersky.com/>.

22 El *malware*, según el Incibe, es un programa informático cuya principal característica es que se ejecuta sin el consentimiento ni autorización del propietario o usuario del equipo infectado y realiza funciones en el sistema que son perjudiciales para el usuario y/o para el sistema. Más detalles en: Instituto Nacional de Ciberseguridad, <https://www.incibe.es/aprendeciberseguridad/>.

Seguridad de la información. Protege la integridad y la privacidad de los datos, tanto en almacenamiento como en tránsito.

Seguridad operativa. Incluye procesos y decisiones para manejar y proteger los recursos de datos.

Recuperación ante desastres y continuidad de actividades. Definen la forma en que una institución responde a un incidente de ciberseguridad o a cualquier otro evento que cause un paro de actividades o pérdida de datos.

Capacitación del usuario final. Aborda el factor de ciberseguridad más imprescindible: las personas. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro.

Partiendo de lo anterior, conviene señalar que, en cualquiera de los casos, se trata de ataques a la seguridad e integridad de las organizaciones y sus sistemas de información, ataques que son tipificados como delitos informáticos, los cuales²³ se realizan por medio de un sistema²⁴ que hace uso de las tecnologías de la información o un componente de éste, que lesiona la integridad, disponibilidad o confidencialidad de la información.

Por su parte, el BCM Institute, en su glosario internacional,²⁵ define la ciberseguridad como el conjunto de herramientas, políticas, directrices, métodos de gestión de riesgos, acciones, formaciones, prácticas idóneas, garantías y tecnologías que puedan utilizarse

23 Fred L. Clark, "Generalidades de la regulación en ciberseguridad".

24 Entiéndase como sistema a todo dispositivo aislado o conjunto de dispositivos, interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos. Para conocer más sobre delitos informáticos y sistemas, se recomienda consultar el documento de trabajo denominado: Generalidades de la regulación en ciberseguridad en los estados miembros de la Comisión de Telecomunicaciones de Centroamérica, disponible en: <https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2015/0910-PA-IXP/6%20Viernes%20SIT%20Clark%20Generalidades%20Regulaci%C3%B3n%20Ciberseguridad.pdf>.

25 BCMpedia del Business Continuity Management Institute: https://www.bcmpedia.org/wiki/Main_Page.

para proteger la disponibilidad, integridad y confidencialidad de la infraestructura conectada, pertenecientes al gobierno, a las organizaciones privadas y a los ciudadanos. Dicha infraestructura incluye componentes físicos y lógicos como los dispositivos informáticos conectados, el personal, las aplicaciones, los servicios, los sistemas de telecomunicaciones, los datos y la información en el mundo cibernético.

Panorama y realidad cibernética en México

El Departamento de Sistemas de American Chamber Mexico²⁶ realizó un estudio minucioso con los resultados obtenidos de la *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares*,²⁷ en el que se destaca que, en México, cada vez hay más usuarios de internet que realizan más operaciones comerciales en línea e intercambian mayor información.

De manera particular, el estudio permitió identificar cuáles son los problemas más comunes que enfrentan los usuarios de internet, encontrando un vínculo directo entre los sistemas de información y la ciberseguridad. A continuación, se muestra un concentrado sobre dichos datos.

Tabla 1. Problemas más comunes que enfrentan los usuarios de Internet en México

Problemática	Número de personas que se ven afectadas	Porcentaje del universo total de usuarios de internet en México
Exceso de información no deseada	20.5 millones de usuarios	25.5 %
Violación a la privacidad	2.5 millones de usuarios	3.1 %
Mensajes de personas desconocidas	16.4 millones de usuarios	20.3 %

26 American Chamber Mexico, “Estrategia de ciberseguridad en México por un futuro ciberseguro”.

27 La encuesta fue realizada por el INEGI y en ella participaron la Secretaría de Comunicaciones y Transportes y el Instituto Federal de Telecomunicaciones. La versión completa de la edición 2019 puede ser consultada en: https://www.gob.mx/cms/uploads/attachment/file/534997/INEGI_SCT_IFT_ENDUTIH_2021.pdf.

Infección por virus	10.6 millones de usuarios	13.1 %
Fraudes con información financiera personal	3.2 millones de usuarios	4.0 %

Fuente: Elaboración propia a partir del informe
“Estrategia de ciberseguridad en México”.²⁸

Tipos comunes de ciberataques

Para la compañía Cisco Systems Inc., un ciberataque es un intento malicioso y deliberado por parte de un individuo o una organización para irrumpir en el sistema de información de otro individuo u organización. Usualmente, el atacante busca algún tipo de beneficio con la interrupción del sistema de información de la víctima.²⁹

El anterior CEO de Cisco, John Chambers, señaló que los ciberataques golpean a las empresas y organizaciones en general, todos los días. Además, refirió que existen dos tipos de empresas: aquéllas que han sido atacadas y aquéllas que no saben que lo han sido. Según el Cisco Annual Cybersecurity Report (CACR), el volumen total de eventos casi se ha cuadruplicado entre enero de 2021 y octubre de 2022.

El equipo de expertos de la misma compañía publicó en su portal web una relación de los ciberataques más comunes hasta ahora detectados:³⁰

Malware. Término que se usa para describir el *software* malicioso, que incluye *spyware*, *ransomware*, virus y gusanos. El *malware* infringe las redes mediante una vulnerabilidad, usualmente cuando un usuario hace clic en un enlace peligroso o en un

28 El informe puede ser consultado a través del siguiente enlace: [https://www.amcham.org.mx/sites/default/files/publications/VF_Estrategia%20de%20Ciberseguridad%20en%20Me%CC%81xico%20\(1\).pdf](https://www.amcham.org.mx/sites/default/files/publications/VF_Estrategia%20de%20Ciberseguridad%20en%20Me%CC%81xico%20(1).pdf).

29 Cisco, “¿Cuáles son los ciberataques más comunes?”.

30 La descripción detallada de los ciberataques más comunes detectados por Cisco Inc. puede ser consultada en: https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html#~how-cyber-attacks-work.

archivo adjunto de correo electrónico que, luego, instala un *software* riesgoso.

Suplantación de identidad (phishing). Es la práctica de enviar comunicaciones fraudulentas que parecen provenir de fuentes confiables, habitualmente a través del correo electrónico. El objetivo es robar datos sensibles, como información de inicio de sesión y tarjetas de crédito, o instalar *malware* en la máquina de la víctima.

Ataque de intermediario. También conocidos como ataques de escucha secreta, ocurren cuando los ataques se insertan en transacciones entre dos partes. Una vez que los atacantes interrumpen el tráfico, pueden filtrar y robar datos.

Ataque de denegación de servicio. Satura los sistemas, los servidores o las redes con tráfico para agotar los recursos y el ancho de banda. Como resultado, el sistema no puede completar las solicitudes legítimas. Los atacantes además pueden usar múltiples dispositivos comprometidos para lanzar un ataque. Se conoce también como ataque por denegación de servicio distribuido (DDoS).

Inyección de SQL.³¹ Sucede cuando un atacante inserta un código malicioso en un servidor que usa el SQL y fuerza al servidor para que revele información que normalmente no revelaría. El atacante puede efectuar la inyección de SQL simplemente enviando un código malicioso a un cuadro de búsqueda de un sitio web vulnerable.

Ataques de día cero. Puede impactar después del anuncio de una vulnerabilidad en la red, pero antes de que se implemente un parche o solución. Los atacantes apuntan a la vulnerabilidad divulgada durante esta ventana de tiempo. La detección de amenazas a la vulnerabilidad de día cero requiere de atención constante.

Tunelización de DNS. Usa el protocolo DNS para comunicar tráfico que no pertenece al DNS por el puerto 53. Envía HTTP y otro tráfico del protocolo por el DNS. Hay varias razones legítimas para

31 SQL, del inglés Structured Query Language, que en español se traduce como Lenguaje de Consulta Estructurado. Para conocer más, se recomienda consultar el sitio: <https://aws.amazon.com/es/what-is/sql/>.

usar la tunelización de DNS. Sin embargo, también existen motivos maliciosos para usar los servicios de VPN de tunelización de DNS. Pueden usarse para encubrir tráfico saliente del DNS y ocultar datos que típicamente se comparten mediante una conexión a internet.

En ese mismo sentido, la compañía multinacional IBM³² publicó también en su portal web su propia clasificación y denominación de los ciberataques más comunes:

Troyano de puerta trasera. Crea una vulnerabilidad de puerta trasera en el sistema de la víctima, lo que permite al atacante obtener control remoto, prácticamente por completo. El troyano suele utilizarse para conectar un grupo de ordenadores de las víctimas a una *botnet* o red zombi, pero los atacantes pueden utilizarlo para otros ciberdelitos.

Ataque de script entre sitios (XSS). Insertan código malicioso en un sitio web legítimo o *script* de aplicación para obtener la información de un usuario, a menudo utilizando recursos web de terceros.

Denegación de servicio (DoS). Inundan los recursos de un sistema, abrumándolos e impidiendo las respuestas a las solicitudes de servicio, lo que reduce la capacidad de ejecución del sistema. A menudo, este ataque sirve para preparar otro ataque.

Túnel DNS. Los ciberdelincuentes utilizan el túnel DNS, un protocolo de transacciones, para intercambiar datos de aplicación, como datos de extracciones, de forma silenciosa o establecer un canal de comunicación con un servidor desconocido, como un intercambio de mandato y control.

Programas maliciosos (malware). Es *software* malicioso que puede inhabilitar los sistemas infectados. La mayoría de las variantes de *malware* destruyen datos eliminando o limpiando archivos críticos para la capacidad de ejecución del sistema operativo.

Phishing. Las estafas de *phishing* intentan robar las credenciales de los usuarios o datos confidenciales, como números de tarjeta

32 IBM, “¿Cuáles son los tipos de ciberataques más comunes?”.

de crédito. En este caso, los estafadores envían a los usuarios correos electrónicos o mensajes de texto diseñados para parecer que provienen de una fuente legítima, utilizando hipervínculos falsos.

Ransomware. Se trata de *malware* sofisticado que se aprovecha de las debilidades del sistema, utilizando cifrado potente para retener datos o la funcionalidad del sistema como rehén. Los ciberdelincuentes utilizan *ransomware* para exigir el pago a cambio de liberar el sistema. Una práctica reciente en el *ransomware* es la aplicación de tácticas de extorsión.

Inyección SQL. Los ataques de inyección SQL (Structured Query Language) insertan código malicioso en aplicaciones vulnerables, generando resultados de consulta de base de datos de *backend* y ejecutando mandatos o acciones similares que el usuario no ha solicitado.

Explosión de día cero. Aprovechan las debilidades de *hardware* y *software* desconocidas. Estas vulnerabilidades pueden existir durante días, meses o años antes de que los desarrolladores descubran los fallos.

En los sistemas de información

Garantizar la integridad de la información es una de las tareas más complejas de cualquier organización ya sea pública o privada, sin embargo, es también uno de los aspectos más vulnerables debido a que estas entidades priorizan la automatización de sus procesos con el objetivo de agilizar las tareas administrativas y optimizar la recolección y sistematización de datos, sin establecer políticas o procedimientos que permitan verificar que toda la información fue almacenada correctamente en el sistema de información y lo más importante, que ésta haya sido registrada en forma precisa y coherente.

El hecho que se generen problemas de integridad de la información representa una fuerte amenaza debido a que exhibe y extiende cualquier vulnerabilidad dentro de la organización, situación que, sin duda, afecta de manera significativa a distintos activos vitales de la misma y genera además problemas severos que se

agudizan gradualmente. En el contexto organizacional, contar con información sensible y pública es un riesgo necesario, debido a que la integración de sistemas de información genera nuevos problemas de seguridad que deben ser atendidos con alta prioridad.³³

En ese sentido, referirnos a temas sobre seguridad de la información representa, necesariamente, considerar la preservación de los principios básicos de confidencialidad, integridad y disponibilidad de la misma y de los sistemas implicados en su tratamiento. Estos tres principios se definen de la siguiente manera:

Confidencialidad. Acceso a la información por parte únicamente de quienes estén autorizados.

Integridad. Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad. Acceso a la información y los sistemas de tratamiento de ésta por parte de los usuarios autorizados cuando lo requieran.

Vale la pena señalar que, en la seguridad de la información, no sólo intervienen los aspectos tecnológicos, sino también una serie de procesos, políticas y procedimientos, ambientes y contexto como centros de cómputo, ubicación de oficinas, y, principalmente, las personas que intervienen los sistemas de información a través de diferentes perfiles de usuario y sus respectivos permisos.³⁴

Es indudable que la tecnología llegó para revolucionar la manera de hacer las cosas tanto en la cotidianidad como a nivel empresarial, haciendo que los procesos se reinventen y se vuelvan más eficientes. De igual manera, resulta innegable que uno de los procesos que más se ha impactado es el proceso de comunicación, donde la información dejó de llevarse de manera física, para ser digitalizada y almacenada en diferentes sistemas de información, dispositivos y en ambiente web, haciendo que se generen riesgos frente a su seguridad y los datos puedan ser vulnerados.

33 I. Gallardo-Bernala, "Ataques Informáticos Basados en la Integridad de la Información", 47.

34 A. Angarita, "Definición de un modelo de medición de análisis de riesgos de la seguridad de la información", 76.

Por lo anterior, las organizaciones, en general, requieren fortalecer sus procesos con la incorporación de herramientas tecnológicas que además de proveer rapidez, flexibilidad y oportunidad a los usuarios, garanticen la protección de la información que se intercambia.

Debe reconocerse que falta camino por recorrer para alcanzar altos estándares en la seguridad de la información y en la reducción del papeleo que ha sido característico del sector público. Asimismo, es importante que se apunte al desarrollo de competencias digitales entre la ciudadanía en general, al igual que la creación de estrategias que permitan atraer y desarrollar talento humano creativo y con conocimientos específicos, que aporten al desarrollo de los procesos de innovación tecnológica.

Es importante, además, crear una cultura digital entre la comunidad, que logre que los procesos sean más amigables, reconociendo que la aplicación de la tecnología ya no es una opción, sino un requisito en el camino hacia el logro de organizaciones competitivas que presten servicios de calidad a sus usuarios, y que haga énfasis en que dichos servicios son actores principales en la relación que debe darse entre el Estado y la sociedad, a fin de alcanzar mayores niveles de interacción y fomentar la confianza y transparencia como principios fundamentales en el sector público.³⁵

En documentos electrónicos

En el contexto de la documentación electrónica, hablar de la seguridad informática necesariamente implica considerar una serie de elementos de carácter técnico, metodológico, normativo y legal, de manera tal que esta tipología documental pueda ser abordada de manera integral.

Como punto de partida, conviene señalar los distintos procesos que hacen posible su existencia, pasando por diversas etapas, desde la generación hasta el acceso por parte de un usuario final:

35 E. Camargo, "La importancia de la seguridad de la información en el sector público en Colombia", 98.

Creación. Etapa inicial que consiste en la producción del documento electrónico o digital, a partir de la necesidad de disponer del testimonio de un hecho o acto específico, y que dé cuenta de lo sucedido. Su generación podrá darse mediante la utilización de un lenguaje natural (convencional) o especializado. Es posible crear documentos electrónicos nativos, o bien, a través de procesos de conversión de soporte análogo a digital.

Edición. Conjunto de acciones encaminadas a la modificación de los archivos, con el propósito de mejorar su presentación y prepararlos para su publicación, distribución o difusión.

Protección. Implementación de medidas de seguridad adicionales para restringir o autorizar su uso. Comúnmente, suelen añadirse marcas de agua en modo imagen o texto, asignarse distintas contraseñas de lectura o escritura, incorporación de firma digital, así como la encriptación de documentos.

Descripción. Proceso técnico-archivístico que permite identificar, analizar y determinar las características internas (contenidos) y externas (formato, peso, medio de almacenamiento, requerimientos para su consulta, etcétera) de los documentos. Esta actividad habrá de estar apoyada con el uso de modelos estructurados y normalizados a través de esquemas que permitan identificar contenido, contexto y estructura, como los metadatos.

Almacenamiento. Acción que se vincula a la recolección, depósito y registro de archivos electrónicos con fines de preservación o difusión. Habitualmente se utilizan servidores locales o de acceso remoto, discos duros, dispositivos ópticos (discos) o magnéticos (cintas) o bien, servicios en la nube para el resguardo de documentos.

Acceso. Es imprescindible definir una lista de control de acceso a cada documento o grupo de documentos. En este listado se deberán especificar los permisos de los usuarios a nivel de roles particulares y por grupo, y están relacionados con los niveles de seguridad de la información que se establezcan en cada organización. Por lo general, se brinda el acceso a la documentación electrónica por medio de una base de datos, de un sistema de gestión de documentos o bien, a través de un repositorio institucional.

Uso y reutilización. Toda vez que los documentos electrónicos han pasado por las tareas y procesos previamente descritos, estarán en condiciones óptimas para su consulta por parte del usuario final, el cual podrá ser una persona física o jurídica, con fines comerciales o no comerciales, todo ello dependiendo del sector, público o privado, al que pertenezca dicha documentación.

CONCLUSIONES

En busca de disminuir el riesgo latente en materia de seguridad informática en los sistemas de información, conviene reflexionar en tres aspectos de gran relevancia que, atendidos de manera oportuna, permitirán asegurar el éxito en las operaciones del propio sistema, así como de los documentos e información que lo integran.

El primer aspecto por considerar corresponde a la gestión documental, tarea que representa un factor clave, que, necesariamente habrá de ser atendida por personal profesional especializado en la materia, además de incorporar procesos encaminados a la certificación a través de la aplicación de estándares internacionales como la Norma ISO 15489.

El siguiente elemento importante para tomar en cuenta son los usuarios vinculados al sistema de información, mismos que deberán estar certificados en los distintos procesos y tareas concernientes al manejo y administración del propio sistema. Conviene hacer mención que los permisos y privilegios de acceso para cada usuario habrán de ser autorizados por un equipo multidisciplinario, multitarea y multinivel de la organización, de manera tal que se garantice con ello, por un lado, seguridad de la información, y por otro, niveles óptimos en materia de transparencia y legalidad sobre el uso y aprovechamiento de sus recursos de información.

Vale la pena mencionar otro de los factores imprescindibles en este tema y que contribuyen a elevar los niveles de seguridad informática en los sistemas de información: nos referimos a los recursos tecnológicos, los cuales deberán estar perfectamente declarados en un manual de organización y definidos con toda

claridad en las políticas y procedimientos por parte del personal responsable en la organización. Invariablemente, se deberán delinear aspectos imperativos en relación con la seguridad perimetral de los sistemas de cómputo, tanto a través de *software* como de *hardware*, programar y realizar respaldos de información de manera periódica, en la medida de lo posible, disponer de servidores espejo, así como la contratación de servicios de antivirus y desinfección que brinden protección a las diversas plataformas, sistemas de información y dispositivos de la organización.

Es evidente la importancia que han alcanzado los sistemas de información en las organizaciones, en primer término, por la gran capacidad de respuesta que brinda a los usuarios en distintos procesos de la gestión documental, además, porque resulta una herramienta de gran trascendencia para la toma de decisiones por parte de directivos y funcionarios, gracias a la amplitud y variedad de documentos e información que poseen, sin embargo, resulta imperante fomentar su planeación y desarrollo con apego a una serie de criterios y lineamientos como los aquí expuestos.

BIBLIOGRAFÍA

American Chamber Mexico. “Estrategia de ciberseguridad en México por un futuro ciberseguro”, consultado el 10 de agosto de 2023. [https://www.amcham.org.mx/sites/default/files/publications/VF_Estrategia%20de%20Ciberseguridad%20en%20Me%CC%81xico%20\(1\).pdf](https://www.amcham.org.mx/sites/default/files/publications/VF_Estrategia%20de%20Ciberseguridad%20en%20Me%CC%81xico%20(1).pdf).

Angarita, A. A., C. A. Tabares, y J. I. Rios. “Definición de un modelo de medición de análisis de riesgos de la seguridad de la información aplicando lógica difusa y sistemas basados en el conocimiento”. *Entre Ciencia e Ingeniería* 9, núm. 17 (2015): 71-80. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-83672015000100010&lng=en&tlng=es.

- Apache HTTP Server Project. "What is the Apache HTTP Server Project?", consultado el 1 de septiembre de 2023. https://httpd.apache.org/ABOUT_APACHE.html.
- Aretio Bertolín Javier. *Seguridad de la información: redes, informática y sistemas de información*. Madrid: Paraninfo Cengage Learning, 2008.
- Arjonilla Domínguez, Sixto Jesús, y José Aurelio Medina Garrido. "La gestión de los sistemas de información en la empresa: teoría y casos prácticos". España: Ediciones Pirámide, 2013.
- BCM Institute. "Business Continuity Management Institute", consultado el 6 de agosto de 2023. <https://www.bcm-institute.org/>.
- Bodero Poveda, E. M., M. R. de Giusti, y C. Morales. "Preservación digital a largo plazo: estándares, auditoría, madurez y planificación estratégica". *Revista Interamericana de Bibliotecología* 45, núm. 2 (2022): 1-14. <https://doi.org/10.17533/udea.rib.v45n2e344178>.
- Camargo, E., A. Ramírez, y M. A. Pinzon. "La importancia de la seguridad de la información en el sector público en Colombia". *Revista Ibérica de Sistemas e Tecnologías de Informação*, núm. 46 (2022): 97-99. <https://doi.org/10.17013/risti.46.87-99>.
- Centro de Información y Documentación Científica (CIN-DOC). "Proyecto UNE-ISO 15489/1. Información y documentación. Gestión de documentos. Parte 1: Generalidades". *Revista Española de Documentación Científica* 28, núm. 1 (2005): 87-116. <https://redc.revistas.csic.es/index.php/redc/article/view/244>.
- Cisco. "¿Cuáles son los ciberataques más comunes?", consultado el 12 de agosto de 2023. https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html.

- Clark, Fred L. “Generalidades de la regulación en ciberseguridad en los Estados Miembros de Comtelca”, consultado el 3 de agosto de 2023. <https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2015/0910-PA-IXP/6%20Viernes%20SIT%20Clark%20Generalidades%20Regulaci%C3%B3n%20Ciberseguridad.pdf>.
- CSIC, CINDOC. “Información y documentación. Gestión de Documentos. ISO/TR 15489-2”. *Revista Española de Documentación Científica* 29 (1): 91-152. <https://redc.revistas.csic.es/index.php/redc/article/view/297>.
- Díaz Jiménez, A., D. Olivera Batista, e I. Zamora Gómez. “Componentes para la conformación de políticas de gestión documental para universidades”. *Información, cultura y sociedad: revista del Instituto de Investigaciones Bibliotecológicas* 47 (2022): 79-92. <https://www.redalyc.org/articulo.oa?id=263073153003>.
- Dungeon of Bits (página web). “Instalación de LAMP”, 24 de octubre de 2019. <https://dungeonofbits.com/instalacion-de-lampapache-mysql-o-mariadb-y-php-sobre-linux.html>.
- Gallardo-Bernal, I. “Ataques Informáticos Basados en la Integridad de la Información”. *Salud y Administración* 2, núm. 5 (Ago 2015): 43-50. https://www.unsis.edu.mx/revista/doc/vol2num5/A4_Atiques_Info.pdf.
- IBM. “¿Cuáles son los tipos de ciberataques más comunes?”, consultado el 19 de agosto de 2023. <https://www.ibm.com/es-es/topics/cyber-attack#:~:text=Pueden%20causar%20valiosos%20tiempos%20de,del%20servici%C3%B3n%20y%20p%C3%A9rdidas%20financieras>.
- . “Diseño físico de la base de datos”, consultado el 13 de agosto de 2023. <https://www.ibm.com/docs/es/db2-for-zos/11?topic=relationships-physical-databases-design>.

INEGI. Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares, 2019. https://www.gob.mx/cms/uploads/attachment/file/534997/INEGI_SCT_IFT_ENDUTIH_2021.pdf.

ISO. “NORMA ISO 27001”, consultado el 20 de agosto de 2023. <https://normaiso27001.es/>.

———. “Norma ISO 27032”, consultado el 20 de agosto de 2023. <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27032:ed-2:v1:en>.

Joyanes Aguilar, Luis. *Sistemas de información en la empresa: el impacto de la nube, la movilidad y los medios sociales*. México: Alfaomega grupo editor, 2015.

Kaspersky. “¿Qué es la ciberseguridad?”, consultado el 15 de agosto de 2023. <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>.

MySQL, consultado el 1 de septiembre de 2023. <https://www.mysql.com/>.

PHP, consultado el 1 de septiembre de 2023. <https://www.php.net/manual/es/intro-what-is.php>.

Santaella, Jesús. “Sistema operativo Linux. ¿Cuáles son sus principales ventajas y desventajas?”, consultado en septiembre de 2023, <https://economia3.com/sistema-operativo-linux/>.

Zambrano Plúa, I. E., E. M. Quindemil Torrijo, y León F. Rumbaut. “Gestión documental en universidades: Una mirada desde Latinoamérica”. *Revista de Ciencias Humanísticas y Sociales* 6, (2021): 108-119. <https://www.redalyc.org/articulo.oa?id=673171216010>.

Información y datos en tiempos de pospandemia. Investigación, docencia y práctica profesional. Vol. 1.

Instituto de Investigaciones Bibliotecológicas y de la Información/UNAM. Edición digital. Coordinación editorial: Angélica Valenzuela; revisión especializada: Marcos Emilio Bustos Flores; corrección de pruebas: Carlos Ceballos Sosa y Marcos Emilio Bustos Flores; formación editorial: Mario Ocampo Chávez. Apoyo en la compilación: Diana Isela Hurtado González. Versión digital: Héctor González Villatoro. Se publicó en junio de 2025.