TLATEMOANI
Revista Académica de Investigación
Editada por Eumed.net
No. 31 – Agosto 2019.
España
ISSN: 19899300
revista.tlatemoani@uaslp.mx

Fecha de recepción: 03 de abril de 2019
Fecha de aceptación: 30 de julio de 2019

CIBERSEGURIDAD Y VIGILANCIA TECNOLÓGICA: UN RETO PARA LA PROTECCIÓN DE DATOS PERSONALES EN LOS ARCHIVOS

AUTORES:

Juan Miguel Castillo Fonseca
miguel.castillo@uaslp.mx

Beatriz Zavala Juárez
archivos_beatriz@hotmail.com

Facultad de Ciencias de la Información
Universidad Autónoma de San Luis Potosí-México.

RESUMEN

El desarrollo de la archivística en México, es un reto que los profesionales de la información deben asumir, aunado con el desarrollo de las tecnologías de la información, en donde no solo basta organizar archivos y ordenar la información, sino conservarla y difundirla a través de medios tecnológicos, a fin de cumplir con iniciativas para un Gobierno abierto, moderno y cercano, de una sociedad de la información y de eliminar la brecha digital entre los ciudadanos y el Gobierno. En este escenario deben considerarse las políticas públicas internacionales como la Agenda 2030, Normas ISO, leyes internacionales de transparencia y acceso, entre

otras; en México, a partir del Plan Nacional de Desarrollo 2013-2018, de la Estrategia Digital Nacional y desde la misma Ley General de Protección de Datos Personales, existen lagunas importantes respecto al uso y protección de datos personales sensibles, principalmente en lo relacionado con ciberseguridad y vigilancia tecnológica.

PALABRAS CLAVE: Ciberseguridad, protección de datos, archivos, seguridad de la información, vigilancia tecnológica, México.

SUMMARY

The development of archives in Mexico is a challenge that information professionals must assume, combined with the development of information technologies, where not only is it enough to organize archives and organize information, but also to conserve and disseminate it through technological means, in order to comply with initiatives for an open, modern and close Government, of an information society and to eliminate the digital divide between citizens and the Government. In this scenario, international public policies such as the 2030 Agenda, ISO Standards, international transparency and access laws, among others, should be considered; in Mexico, from the 2013-2018 National Development Plan, the National Digital Strategy and from the General Law for the Protection of Personal Data, there are important gaps regarding the use and protection of sensitive personal data, mainly related to cybersecurity and technological surveillance.

KEYWORDS: Cybersecurity, data protection, archives, information security, technological surveillance, Mexico.

1. INTRODUCCIÓN

La democracia entendida en una idea muy abstracta (Castillo Fonseca, J.M. 2016)[1] es considerada como una forma de gobierno del Estado, en donde su principal

[1] CASTILLO FONSECA, J.M. (2016), “La estructuración de sistemas de gestión de documentos y archivos como base para la implementación de un sistema de preservación digital.” Cuadernos de

característica es que el poder es ejercido por los ciudadanos o el pueblo, mediante mecanismos de participación en la toma de decisiones, por lo cual, existiendo sistemas con información accesibles, transparentes y que permitan la interacción ciudadana, se consideraría una forma democratizar la información del Gobierno hacía la sociedad.

Los archivos en México, representan a través de su gestión documental, el cúmulo de funciones y actividades que el Gobierno realiza día a día con la finalidad de cumplir sus obligaciones ante los ciudadanos, mediante la gestión pública.

La Estrategia Digital Nacional (EDN), es el plan de acción que el Gobierno de la República ha implementado, para fomentar la adopción y el desarrollo de las Tecnologías de la Información y la Comunicación (TIC) e insertar a México en la Sociedad de la Información y el Conocimiento. Dicha estrategia surge en el marco del Plan Nacional de Desarrollo (PND) 2013-2018, y forma parte de la estrategia transversal “Gobierno Cercano y Moderno”.

La idea es aumentar la digitalización en México, para que con ello se maximice su impacto económico, social y político en beneficio de la calidad de vida de las personas, sin embargo, aún existe un grave letargo en:

1. **Materia archivística.** Falta de Organización documental en muchas dependencias.
2. **Aplicación de Tecnologías.** No existe inclusión de esquemas de preservación digital.
3. **Lagunas legales**. Referentes a la protección de datos personales en posesión de los sujetos obligados.
4. **Ciberseguridad y Vigilancia tecnológica.** Falta de medidas de protección en las administraciones.

Investigación de Ciencias de la Información. No. 1, 2016. 40 p. [Consultado: 5 de marzo de 2019] [en línea] http://cuinci.org/index.php/cuinci/article/view/5

5. **Políticas públicas**. Que permitan desarrollar esquemas y protocolos en caso de robo de datos personales y hackeo de información.
6. **El papel de las instituciones responsables.** INAI, AGN, Secretaría de la Función Pública, Secretaría de Gobernación, Secretaría de Seguridad Pública, el Instituto Federal de Telecomunicaciones, el propio Sistema Nacional Anticorrupción, entre otros.
7. **Otras.**

Incluso la Ley General de Archivos fomenta a considerar en tres de sus objetivos básicos (MÉXICO. Ley General de Archivos. 2019)[2] lo siguiente:

- Regular la organización y funcionamiento del Sistema Institucional de Archivos de los sujetos obligados, a fin de que éstos se actualicen y permitan la publicación en medios electrónicos de la información relativa a sus indicadores de gestión y al ejercicio de los recursos públicos; y de aquella que por su contenido sea de interés público.
- Establecer el uso y aprovechamiento de tecnologías de la información para mejorar la administración de los archivos.
- Definir las bases para el desarrollo y la implementación de un sistema integral de gestión de documentos electrónicos encaminado al establecimiento de gobiernos digitales y abiertos en el ámbito federal, estatal y municipal.

La pregunta es ¿México está preparado para afrontar la responsabilidad del uso y manejo de los datos personales, a través de las tecnologías de la información? Por lo anterior, el objetivo de este trabajo es analizar los conceptos e importancia de la protección de datos personales, la ciberseguridad y la vigilancia tecnológica desde la perspectiva archivística y cómo los profesionales de la información debemos estar preparados para estos retos en la salvaguarda de dichos datos personales en posesión de los sujetos obligados, que están en los archivos públicos o privados.

[2] MÉXICO. Ley General de Archivos. DOF. 15 de junio de 2019. 2 p.

La metodología empleada en esta investigación, se basa en un método analítico de fuentes documentales.

2. Protección de datos personales

Los datos personales consisten en toda aquella información que puede ser relacionada con una persona y permite identificarla. Algunos datos pueden ser la edad, domicilio, número telefónico, correo electrónico, historial académico o profesional, patrimonio, número de seguro social, CURP, estado de salud, ideología religiosa, política o filosófica, preferencias sexuales, etc. Dentro de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados divide los datos personales en 2 categorías:

1. Artículo 3. Frac. IX. Dato personal: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información. (México, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017) [3]

2. Artículo 3. Frac. X. Dato personal sensible: son aquellos a que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De forma enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y

[3] MÉXICO. DOF. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. 26 de enero de 2017. 2 p.

> preferencias sexuales. (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017)[4].

En México, la protección a los datos personales se encuentra reconocida como una garantía individual dentro del artículo 16° constitucional que menciona:

> Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde o motive la causa legal del procedimiento.
> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la Ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros […] (México, Constitución Política de los Estados Unidos Mexicanos, 2017)[5]

Los cambios vertiginosos a los que los profesionales de la información se enfrentan como una consecuencia de los avances y generación de nuevas tecnologías, proporcionando ventajas gracias a que con la utilización de ellas se puede realizar el intercambio de la información, pero a la vez implican un reto al momento de garantizar la protección de los datos personales.

Con la aprobación de la Ley General de Protección de Datos en Posesión de Sujetos Obligados (LGPDPSO) el 13 de diciembre del 2016 y publicada el 26 de enero de 2017, lo más relevante de la ley general con diferencia de la federal es que esta se eleva a rango de Ley General generando que los entes del sector público y privado

[4] MÉXICO. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. DOF. 2017, 2 p.
[5] MÉXICO, Constitución Política de los Estados Unidos Mexicanos. DOF. 2017, 15 p.

deberán observar casi lo mismo, basándose en los principios que se muestran en la siguiente imagen.

Ilustración 1. Principios en el tratamiento de Datos Personales

Creación de los autores.

Con el establecimiento de esta Ley, las instituciones del Sector Público deberán establecer las medidas de seguridad que contribuyan a evitar la alteración, pérdida, transmisión o acceso no autorizado de los datos recabados, teniendo especial cuidado e incrementando la seguridad cuando se trate de información de carácter sensible.

Además, exige contar con un documento de seguridad que consiste en un instrumento a través del cual se describe y da cuenta sobre las medidas técnicas, físicas y administrativas que deben ser adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos que tienen bajo su resguardo.

La institución debe generar procesos para su conservación, bloqueo y supresión de los datos personales, estableciendo periodos de tiempo para su conservación. Entre los procesos que deben ser implementados, se encuentra el establecimiento de

auditorías internas y externas, con lo cual, se podrá vigilar el cumplimiento de la protección de la información.

También debe realizarse una evaluación de impacto a la privacidad, la cual consiste en un documento mediante el cual se señala que se pretende poner en operación, modificar algún sistema o plataforma informática, políticas aplicaciones electrónicas o cualquier tecnología que implique el tratamiento de datos personales.

Como resultado de esta evaluación deben valorarse los impactos a efecto de identificar y mitigar posibles riesgos que puedan presentarse, y/o se encuentren relacionados con los principios, deberes y derechos de los titulares el organismo. Dicha evaluación es presentada al Instituto Nacional de Acceso a la Información (INAI) quien podrá emitir algunas recomendaciones.

Por último, los organismos deben contar con un sistema de borrado seguro de la información que poseen a su cargo, el cual permita garantizar el ejercicio de los Derechos ARCO (Acceso, Rectificación, Cancelación u Oposición) al momento de recibir una solicitud de información al respecto.

3. Ciberseguridad

Es pertinente contextualizar la diferencia conceptual entre seguridad de la información y ciberseguridad, debido a que son términos que a pesar de ser manejados de forma similar implican diferente significado:

La **Ciberseguridad** de acuerdo con la ISACA (*Information Systems Audit and Control Association*) la define como:

> Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada,

almacenada y transformada por los sistemas de información que se encuentran interconectados. (Mendoza, 2015)[6].

Mientras que la **seguridad de la información**, según la ISO27001 se refiere a la confidencialidad, integridad y disponibilidad de la información y los datos importantes para las organizaciones, independientemente del soporte en que se encuentren, estos pueden estar en soporte electrónico, papel, audio y vídeo.

La falta de políticas y controles de seguridad por parte de los individuos ocasionan graves riesgos debido a que la información confidencial no se encuentra protegida, permitiendo que circule libremente o sea vendida al mejor postor para fines desconocidos.

El Hackeo de información es uno de los principales problemas que se presentan en el entorno digital, tal es el caso del cierre de la **plataforma japonesa Mt.Gox** (Expansión, 2014) mostrando que los hackeos se pueden presentar en cualquier momento y ocasionar daños irreparables. Esta era una de las mayores operadoras de bitcoins del mundo, pero el conjunto de diversos problemas como: mala gestión de la compañía, los pésimos sistemas de seguridad, la falta de transparencia, la falta de controles, la poco regulación interna y la pérdida de 400 millones de dólares en bitcoins dio como resultado que el hackeo de la información por parte de ciberdelincuentes ocasionará al desmoronamiento y extinción de la empresa.

Para el 22 de octubre del 2016, un **Banco Brasileño** tuvo un ataque cibernético en donde se editaron 36 registros de su DNS (Domain Name System) a través del cual se enruta toda la información de todo el Banco a un clon, a un phishing[7] global

[6] MENDOZA, M. A. Welivesecurity. (2015). ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia. Fecha de publicación: 16 de junio de 2015. [Consultado: 25 de enero 2019] [En línea] https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

[7] El **phishing** es una táctica usada por cibercriminales y estafadores para robar tu información personal. A través de correos electrónicos engañosos, mensajes de texto, alertas de mensajería instantánea, entre otros, buscan robar tu información financiera como números de tarjetas de crédito, contraseñas, información de cuentas y otros datos.

logrando tener el control del banco alrededor de 6 horas, y aún no se sabe el daño monetario causado por este suceso.

Sin lugar a dudas México, no es la excepción, según la empresa Lockton, en el ranking de los países posiciona en segundo lugar en Latinoamérica en ataques cibernéticos a dispositivos móviles. Es para el mes de junio de 2016 que en la **plataforma gob.mx** se presentaron más de 1 millón de visitas únicas diarias en pocos días ocasionando un ataque volumétrico de la negación del servicio trayendo como resultado que durante 45 minutos no se tuviera acceso a la misma; podría verse como un evento aislado, sin embargo, 3 meses después un ataque masivo vulnera las infraestructuras de **Amazon, Spotify, Twitter, Pagerduty Github, Business Insider, Soundcloud, Heroku, Etsy, Netflix** (El confidencial, 2016) entre algunos otros afectados al mismo tiempo.

Ilustración 2. Interrupciones detectadas a las 9:20 am ET

Imagen tomada de downdetector

Ilustración 3. Interrupciones informadas a las 4:58 pm ET

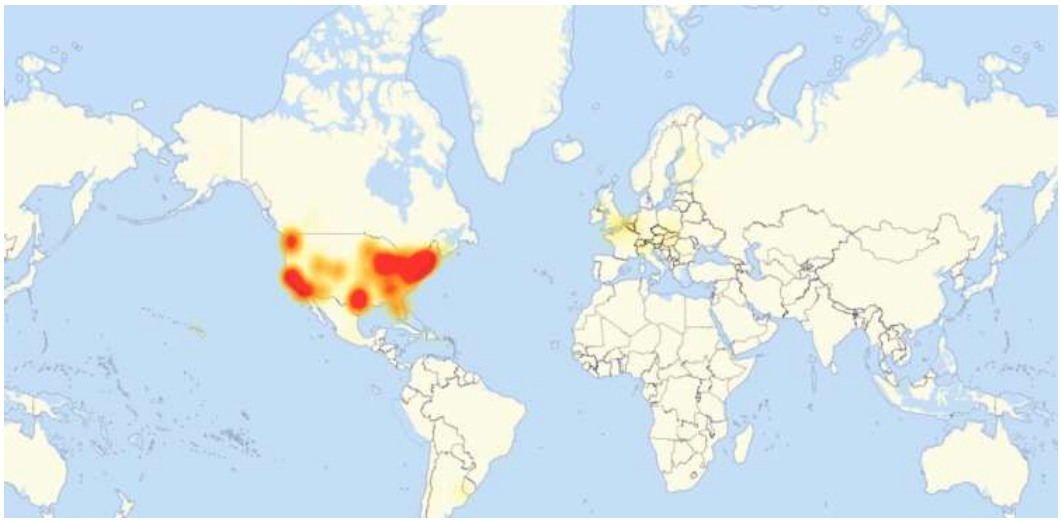


Imagen tomada de downdetector

En los mapas anteriores se muestra el momento en que se realizaban los ataques a gran escala en los EE.UU. Pero el robo de información por ciberdelincuentes es un problema que se ha seguido presentando en las grandes y pequeñas empresas, ONG´s, independientemente del sector público o privado.

Otro caso se presentó en **Equifax,** una agencia de crédito financiero encargada de recopilar información de diferentes entidades, con la cual influía en el comportamiento positivo y negativo de personas físicas y morales. Es para julio del 2017, cuando sufre un problema de vulnerabilidad de la información almacenada en su servidor Web, el cual tenía meses de antigüedad, pero debido a que no contaba con parches que contribuyeran a la protección de su servidor se realizó el Hackeo[8] de 143 millones de cuentas de personas en EE.UU., entre los que se encontraban nombres completos, números de Seguro Social, fechas de nacimiento y direcciones postales.

La empresa Equinox declaro que, desde el 6 de marzo del mismo año se había detectado por primera vez con la ayuda de una firma de ciberseguridad una puerta de enlace de hackeo, por lo que en menos de una semana se implantaron los

[8] **Hackear es un término que ha ganado muchos significados en los últimos años.** Se utiliza para hablar de **todo acto relacionado con la piratería,** como puede ser desde realizar un ataque informático a un ordenador a crackear un software para usarlo sin tener su licencia original.

parches para esta vulnerabilidad. Sin embargo, no se tiene certeza de por qué continuo la falla en los servidores, pues el hackeo masivo de su información inicio en el mes de mayo y duro meses sin poder detenerse; siendo revelado este problema meses después hasta el 7 de septiembre. Es sin lugar a dudas uno de más grandes robos de información en los Estados Unidos durante el 2017.

Otro caso fue el suscitado durante el 2018, cuando se realizó la filtración de datos personales de más de 87 millones de cuentas de usuarios de **Facebook** por parte de la consultora Cambridge Analytica, la cual se presentó de la siguiente manera:

> Facebook declaro que un **profesor usó las herramientas de inicio de sesión de Facebook para que la gente se inscribiera en una aplicación de análisis de personalidad** diseñada con fines académicos. Unas 270 mil personas dieron permiso para acceder a los datos a través de Facebook sobre ellos y sus amigos, exponiendo una red de 50 millones de personas, según el New York Times.
> Ese tipo de acceso estaba permitido según las reglas de Facebook en ese momento, pero actualmente los desarrolladores no pueden pedir acceso a datos sobre los amigos de los usuarios. Después, el profesor violó los términos de Facebook cuando pasó esa información a la empresa Cambridge Analytica. (El financiero, 2018)

Ilustración 4. Cambridge Analytica

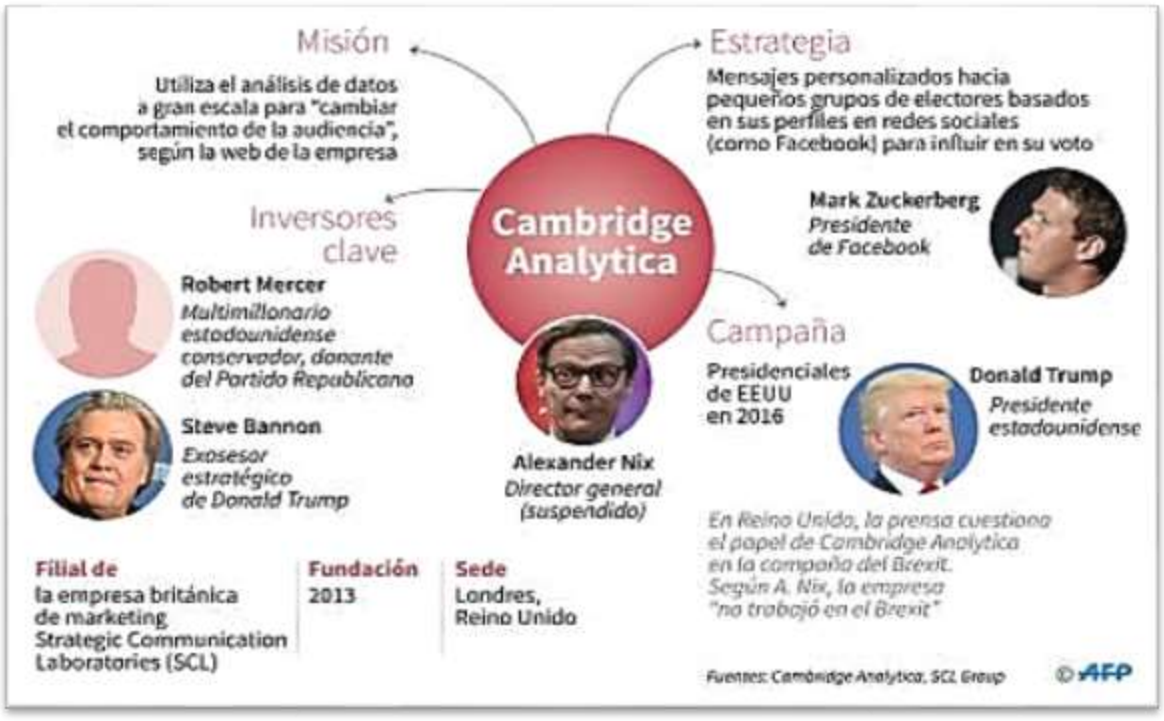
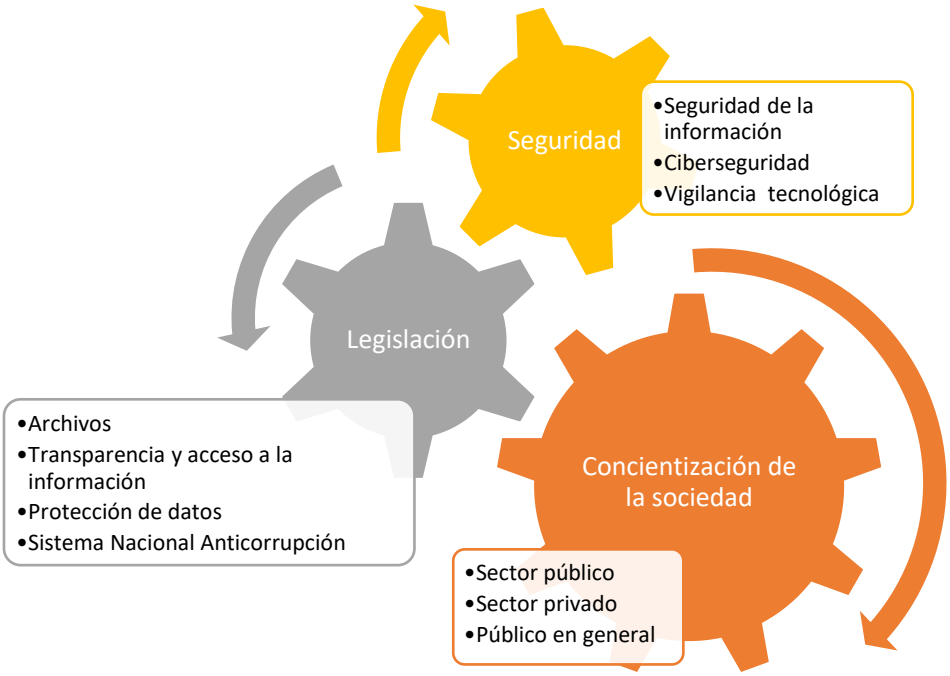


Imagen tomada de El Universal. (El Universal, 2018)

A partir de esta situación, se comenzaron a realizar diversos cambios en la configuración del Facebook en donde los usuarios si así lo prohíben, las compañías no podrán acceder a sus datos personales, número de teléfono, contactos, biometría, entre otros. El tema de la seguridad de la información se ha visto de forma aislada con respecto a la privacidad, debido a que se maneja como si fuera una balanza con la que al ofrecer mayor seguridad se va perdiendo la privacidad y disminuye la protección de los datos personales; sin lugar a dudas estos mecanismos deben ser reflexionados y tratados de forma conjunta a través de una estrategia que considere la concientización de la sociedad al momento de proporcionar sus datos, por lo cual la legislación debe contribuir con normas y políticas para su uso y regulación, además de contemplar los mecanismos y herramientas de seguridad que permitan su protección.

Ilustración 5. Estrategia conjunta de seguridad



Creación de los autores.

Al fortalecer estos tres aspectos se tendrá la obligación por parte del sector público y privado de proporcionar confidencialidad, integridad y disponibilidad de la información, independientemente del soporte o formato en que se encuentren.

4. Vigilancia tecnológica

Muchas instituciones públicas y empresas del sector privado utilizan los portales y aplicaciones web para publicar contenidos de diversos tipos, utilizar el correo institucional, realizar comercio electrónico, incluso para ofrecer un servicio a la población. Sin embargo, esto representa un problema debido a que deja abierta la puerta a los ataques informáticos que puede realizar un ciberdelincuente con la finalidad de comprometer los datos, interrumpir el servicio que se ofrece o realizar un secuestro de la información para conseguir dinero.

La **vigilancia tecnológica**[9] ha sido definida por diversos autores a lo largo de la historia, como se muestra en la siguiente tabla de la descripción histórica del término:

Tabla I. Definiciones de vigilancia tecnológica. (González, 2015: 18-19)

Definición	Autores	Año	País
"La VT es la observación y el análisis del entorno, seguidos por la difusión bien especificada de las informaciones seleccionadas y analizadas, útiles para la toma de decisiones estratégicas"	Francois Jakobiak y Henri Dou	1992	Francia
"La VT incluye todos los esfuerzos que la empresa dedica, los medios de los que se dota y las disposiciones que toma, con el objetivo de conocer todas las evoluciones y novedades que se producen en los dominios de las técnicas que le conciernen actualmente o son susceptibles de afectarle en el futuro".	Humbert Lesca	1995	Francia
"La VT es el arte de descubrir, recolectar, tratar, almacenar informaciones y señales pertinentes, débiles y fuertes, que permitan orientar el futuro y proteger el presente y el futuro de los ataques de la competencia tecnológica. Transfiere conocimientos del exterior al interior de la empresa".	Daniel Rouach	1996	Francia

[9] GONZALEZ Alcalá, A. II y DAVID GÓMEZ, D. (2015). *Guía práctica InnoViTech: Vigilancia Tecnológica para la Innovación.* Servicio Nacional de Aprendizaje, SENA: Rionegro-Antioquia, 2015. 18-19 p. [Consultado: 9 de marzo 2019] [En línea] https://es.slideshare.net/nestorg10/gua-prctica-innovitech-2015

Definición	Autores	Año	País
“La VT consiste en analizar el comportamiento innovador de los competidores directos e indirectos, explorar todas las fuentes de información (Libros, bases de datos, patentes, etc.), examinar los productos existentes en el mercado (tecnología incorporada) y asistir a ferias y congresos para posicionarse respecto a los demás competidores y tomar así conocimiento de las competencias tecnológicas que predominarán en un futuro más o menos próximo. Todo ello sin perder de vista la capacidad tecnológica presente y la que estará en condiciones de desarrollar la empresa para enfrentarse a nuevos retos”.	Patricio Morcillo	1997	España
La VT exige enfoques multidisciplinares y horizontales. Las amenazas y oportunidades que más sorprenden, muchas de ellas de alto impacto para la empresa, suelen provenir de sectores colaterales.	Palop & Vicente, J. M.	1999	Madrid, España
“La VT e IC constituyen un proceso sistemático en el que se capta, analiza y difunde información de diversa índole económica, tecnológica, política, social, cultural, legislativa, mediante métodos legales, con el ánimo de identificar y anticipar oportunidades o riesgos para mejorar la formulación y ejecución de la estrategia de las organizaciones”.	Fernando Palop y J. Sánchez	2002	España
“La VT es una forma sistemática de captación y análisis de información científico-Tecnológica que sirve de apoyo en los procesos de toma de decisiones”.	Sistema Madrid	2009	España
“La VT es el proceso organizado, selectivo y sistemático, para captar información del exterior y de la propia organización sobre ciencia y tecnología, seleccionarla, analizarla, difundirla y comunicarla, para convertirla en conocimiento con el fin de tomar decisiones con menor riesgo y poder anticiparse a los cambios.”	AENOR UNE 16006:2011	2011	España

Definición	Autores	Año	País
La vigilancia tecnológica involucra procesos de planeación, dirección y control, coordinación del desarrollo e implementación de la información para entender y anticiparse a los cambios tecnológicos, haciendo una detección temprano de eventos que representan oportunidades o amenazas potenciales.	Bouza-Betancourt, Gutiérrez-Álvarez, & Raposo-Villavicencio, 2010 Castellanos Domínguez et al.; Moyares Norchales & Infante Abreu, 2016	2010 2016	Cuba

Se puede entender por vigilancia tecnológica al proceso planeado, organizado y sistemático que contribuye a captar información del exterior y de la propia organización, para poder entender y anticipar con ello cambios, oportunidades y amenazas tecnológicas.

Por lo tanto, fundamental que dentro de las organizaciones se apliquen los correctos niveles de ciberseguridad que impidan la vulnerabilidad en los sistemas, aplicaciones web y servidores de las bases de datos a los ciberdelincuentes.

Por ello es necesario involucrar a los directivos en la implementación y seguimiento de los problemas que se presenten y puedan comprometer los datos personales, el prestigio y la credibilidad de la institución en relación a sus medidas de seguridad.

5. Análisis normativo de la protección de datos.

En el siguiente esquema se explica la relación de los elementos que se han presentado a lo largo del artículo, en donde se visualiza de acuerdo a la normatividad empleada desde el ámbito internacional y nacional relacionada con la gestión de los documentos, archivos, protección de datos, estrategias de desarrollo

y la agenda 2030, se observa cómo impacta en los archivos (físicos, digitales y electrónicos).

Tabla II. Análisis normativo de protección de datos

País o institución	Políticas y disposiciones legales	Análisis
Organización de las Naciones Unidas (ONU)	Declaración de los Derechos Humanos 1948	Dentro del artículo 12 el derecho a la protección de los datos con el que cuentan todas las personas.
	Convención americana sobre derechos humanos (Pacto San José) 1969	La Convención americana sobre derechos humanos mejor conocida como "Pacto San José", fue suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos, llevada a cabo en San José de Costa Rica del 7 al 22 de noviembre de 1969.
Alemania	Ley de Protección de Datos (Datenschutz) 1970 Fue cambiada por la *Ley Federal Bundesdaten-schutzgesetz* 1977	Considera la primera ley que permite la protección de datos a nivel mundial. Para el año de 1977 el Parlamento Federal de Alemania aprueba la denominada *Ley Federal Bundesdatenschutzgesetz*. Prohibiéndose la transacción e utilización de cualquier dato personal sin la debida autorización del interesado.
Suecia	1973	Considerada la primera ley en el mundo encargada de proteger la información de los particulares. Esta ley contaba con un organismo supervisor para su cumplimiento (*Data Inspektion Board*).
Estados Unidos de América	Privacy Act 1974	Siendo una ley de carácter general para la protección de la información.

País o institución	Políticas y disposiciones legales	Análisis
Países miembros del consejo de Europa	Convenio 108 o convenio de Estrasburgo 1981	Surge el primer convenio internacional de protección de datos con la participación de Alemania, Francia, Dinamarca, Austria y Luxemburgo. De este modo estos países contaron con el primer instrumento vinculatorio de carácter internacional sobre protección de datos; posteriormente se ingresaron países como Islandia, Gran Bretaña, Irlanda, Holanda, Portugal, España y Bélgica. Para los años 90´s se establece una norma común la cual se denominó *Convenio 108.*
Unión Europea	Directiva 97/66/EC acerca del tratamiento de datos personales y la protección de intimidad en el sector de las telecomunicaciones 1997	La Directiva de EC sobre Protección de Datos (95/46/EC) tiene un doble objetivo: Debería proteger los derechos fundamentales y las libertades, especialmente el derecho a intimidad de personas físicas, en el tratamiento de datos generales; pero también debería reconciliar el nivel variable de protección de datos en los Estados Miembros para que el libre movimiento de bienes, personas, servicios y capital en el mercado interior se garantice. Aparte del Convenio de Protección de Datos más general y menos rigurosamente organizado del Consejo Europeo, la Directiva de EC sobre la Protección de Datos 95/46/EC y la Directiva de Protección de Datos de Telecomunicación 97/66/EC son el único reglamento vinculante de protección de datos bajo derecho internacional.
España	Ley Orgánica 15 1999	La importancia de esta ley radica en que ha servido como referente del modelo europeo para todo Latinoamérica, permitiendo homologar la manera mediante la cual se protejan los datos personales.

País o institución	Políticas y disposiciones legales	Análisis
	ISO 15489 (2001) Familia ISO 30300	Esta norma en conjunto con la familia de las ISO 30300 ofrecen un marco legal para la implementación de un sistema de gestión de documentos.
Rusia	Ley de Protección de Datos Personales 2006	Fue aprobada una exhaustiva de esta Ley.
Perú	Ley 29.733 2011	Se aprueba el 2 de julio del 2011 la Ley de protección de datos personales.
Colombia	Ley 1581 o también conocida como Ley de Protección de Datos Personales 2012	La Ley reconocer y protege el derecho que tienen todas las personas de conocer, rectificar y actualizar su información.
México	Agenda 2030 2015	El 25 de septiembre de 2015 más de 150 líderes mundiales asistieron a la Cumbre de las Naciones Unidas sobre el Desarrollo Sostenible en Nueva York con el fin de aprobar la Agenda para el Desarrollo Sostenible. El documento final, titulado "*Transformar Nuestro Mundo: la Agenda 2030 para el Desarrollo Sostenible*", siendo adoptada por los 193 Estados Miembros de las Naciones Unidas. Este documento cuenta con 17 Objetivos del Desarrollo Sostenible cuya finalidad es poner fin la pobreza, luchar contra la desigualdad y la injusticia, y hacer frente al cambio climático sin que nadie quede rezagado para el 2030.
México	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. 2017	La Ley regula tiene el objeto de establecer las bases, principios y procedimientos para garantizar el derecho de toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

Creación de los autores.

En la tabla anterior, se observa el análisis normativo relacionado con la protección de datos personales a través de la historia, considerando como punto de partida la Declaración de los Derechos Humanos expuesta por la Organización de las Naciones Unidas (ONU]) en el año de 1948, dentro de esta declaración se enuncia por primera vez el derecho a la protección de los datos.

Como se puede observar, la protección de datos personales es un tema importante en las agendas internacionales y en las políticas públicas, sin embargo, es menester activar protocolos de seguridad para la administración de dichos datos con el uso de la tecnología.

6. Propuestas para combatir desde los archivos la protección de datos personales en relación a la Ciberseguridad y la Vigilancia tecnológica.

De acuerdo con lo mencionado anteriormente se pueden tomar algunas medidas dentro de las organizaciones que contribuyan a la seguridad de la información y de los archivos:

- Restringir el acceso a las personas que no formen parte de la organización, así como implementar mecanismos de control para el personal que administra y utiliza la información de la institución y de los archivos físicos como digitales.

- Capacitar y concientizar al personal sobre el manejo y protección de la información a la que tienen acceso.

- Elegir informáticos responsables que conozcan de programación y desarrollen sistemas con mayores niveles de seguridad y no solo adquieran programas informáticos comerciales, que son del conocimiento de los ciberdelincuentes. Es decir que las instituciones contraten personal en informática que desarrolle software, a través de lenguajes de programación y no adquiera cualquier software que vendan empresas, porque generalmente los hackers o

ciberdelincuentes al vulnerar algún software, tendrán acceso a los sistemas de las organizaciones que han adquirido dicho software en particular.

- En otros casos se puede hacer uso de software libre con potencialidad de desarrollo, los cuales requieren también personal en informática que conozca de lenguajes de programación.

- Establecer permisos de acceso con los cuales identificar quien puede visualizar, agregar o modificar la información y que una vez se encuentre terminada los archivos no puedan ser modificados.

- Controlar los procedimientos internos para la utilización de datos, archivos y programas.

- Generar los avisos de privacidad, los cuales deberán estar disponible y al alcance de los usuarios.

- Actualizar de forma constante las contraseñas de los sistemas, generando claves intransferibles.

- Mantener organizada la documentación de la organización conforme a los procesos archivísticos, respetando los principios de procedencia y orden original.

- Controlar la generación de documentos electrónicos a través de las cadenas de custodia o cadenas de valor codificado, como el caso de la norma ISO 15489:2001. Information and Documentation: Records Management: Consiste en una guía para la gestión de documentos de archivo de una organización, sea cual sea su soporte. Esta norma establece que “...los documentos de archivo deben ser auténticos, confiables, completos, sin alteración, y deben permitir su uso y acceso. Asimismo, deben poseer metadatos que definan el

contexto, contenido y estructura y deben reflejar con precisión la comunicación, acción o decisión.” (Voutssás, 2010)[10].

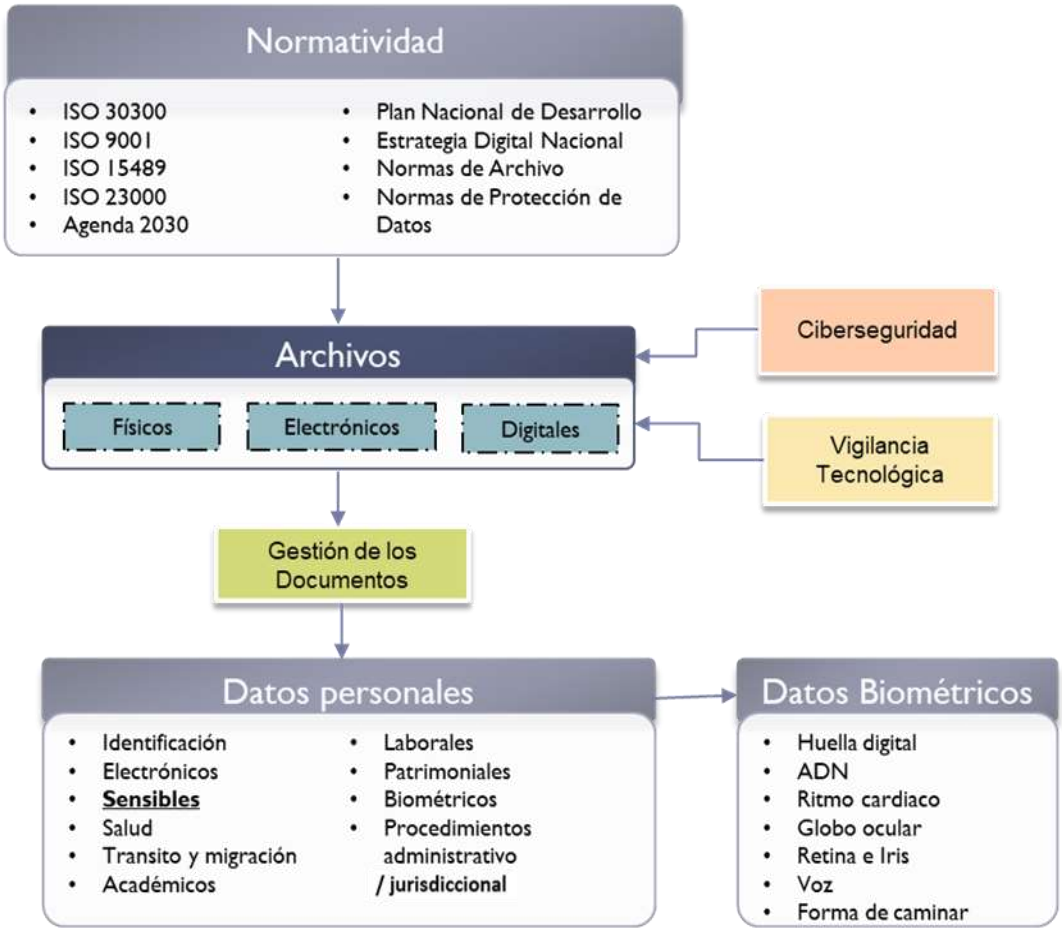
- Considerar los 6 puntos de la cadena de preservación digital, que señala el autor Juan Voutssás (Voutssás, 2010)[11], en donde se ve al documento como un objeto de preservación digital y debe atenderse con las siguientes acciones: 1. Establecer alcance y objetivos, 2. Allegarse de los recursos, 3. Enfocarse en los documentos de archivos digitales, 4. Ofrecer asesoría, 5. Desarrollar procedimientos e 6. Implementar estrategias de conservación documental.

- Generar los instrumentos archivísticos en un sistema de información, a través de bases de datos, la cual mantendrá un control de los documentos, permitiendo saber quién es el responsable de los documentos, así como quien y cuando los consulto

En el siguiente esquema se observa la relación con los temas tratados en este trabajo.

[10] VOUTSSÁS M., Juan. 2010. “Preservación Documental Digital y Seguridad Informática” En: Investigación Bibliotecológica. Centro Universitario de Investigaciones Bibliotecológicas, UNAM. Vol. 24, no. 49. Citado en: Archivos Electrónicos Textos y Contextos. [Consultado: 19 de marzo 2019] [En línea]
http://www.interpares.org/display_file.cfm?doc=ip3_mexico_dissemination_bc_voutsass_archivos-electr%C3%B3nicos_2011.pdf
[11] Ref. 8.

Esquema 1. Relación de archivos, ciberseguridad y vigilancia tecnológica con los datos personales sensibles. (Datos biométricos)



Creación de los autores.

Dentro de los archivos deben considerarse temas relacionados con la vigilancia tecnológica y la ciberseguridad, que a la par de una adecuada gestión de los documentos, permita garantizar la protección de los datos personales, específicamente los clasificados como datos sensibles en donde se encuentra el grupo de los datos Biométricos.

CONCLUSIONES

- Los archivos cada día siguen representando nuevos retos para los profesionales de la información, al implementar los procesos de organización de la información documental, al sistematizar la información, al digitalizar, al difundir y transparentar la información, al conservar y preservar, no solo física, sino ahora con el uso de la tecnología.

- La labor de los archivistas retoma cada vez mayor importancia y relevancia, no cabe duda que en el futuro que nos deviene, la figura de los profesionales de la información, será vital, para seguir preservando la cultura y la historia de las naciones.

- La protección de datos personales en diferentes partes del mundo, desde 1948, ha sido un tema que ha crecido en las agendas internacionales y en las políticas públicas, sin embargo, con el desarrollo de la tecnología, la protección de datos personales relacionados con la ciberseguridad y la vigilancia tecnológica, aún es un tema a regular, a fin de evitar el robo de identidad, el hackeo y el mal uso de la información, entre otros.

- Por último, es importante mencionar que existe un vacío legal en materia de robo de identidad en diferentes partes del Mundo, México ocupa el octavo lugar a nivel Mundial, con más de 50 mil denuncias. (La Jornada. Aguascalientes, 2017)[12]

De acuerdo con Nuala O´Connor, presidente y CEO del Centro para la Democracia y la Tecnología se retoma la siguiente frase “Las tecnologías de comunicación se han convertido en una parte esencial de nuestra vida cotidiana, pero si no podemos

[12] LA JORNADA. (2017). México ocupa el octavo lugar de robo de identidad en todo el mundo con más de 50 mil denuncias. Fecha de publicación: 16 de diciembre de 2017. [Consultado 5 de febrero 2019] [en línea] http://www.lja.mx/2017/12/mexico-ocupa-octavo-lugar-robo-identidad-en-mundo-50-mil-denuncias

controlar nuestros datos, estas tecnologías nos controlan. Para que nuestra democracia prospere, esto no puede continuar". (El financiero, 2018)[13]

BIBLIOGRAFÍA

ARCHIVO GENERAL DE LA NACIÓN. (2018). Ley General de Archivos. México. [Consultado: 6 de marzo 2019] [En línea] https://www.gob.mx/agn/articulos/aprueba-el-senado-de-la-republica-la-ley-general-de-archivos?idiom=e3s

CASTILLO FONSECA, J. M. (2016). "La estructuración de sistemas de gestión de documentos y archivos como base para la implementación de un sistema de preservación digital." *Cuadernos de Investigación de Ciencias de la Información.* No. 1, 39-55 p. [Consultado: 5 de marzo de 2019] [En línea] http://cuinci.org/index.php/cuinci/article/view/5

EL CONFIDENCIAL. (2016*). Un ciberataque masivo inutiliza las grandes páginas web en EEUU y Europa.* Fecha de publicación 21 de octubre de 2016. [Consultado: 5 de febrero 2019] [En línea] https://www.elconfidencial.com/tecnologia/2016-10-21/ciber-ataque-ddos-twitter-facebook_1278793/

EL FINANCIERO. FRIER, S. (2018). *Facebook se hunde en el robo de datos. Fecha de publicación.* 20 de marzo de 2018. Fecha de actualización: 19 de marzo de 2018. [Consultado: 4 de mayo 2018] [En línea] http://www.elfinanciero.com.mx/tech/facebook-se-hunde-por-el-robo-de-datos

[13] EL FINANCIERO. FRIER, Sarah. (2018). Facebook se hunde en el robo de datos. Fecha de publicación: 20 de marzo de 2018. Fecha de actualización: 19 de marzo de 2018. [Consultado: 4 de mayo 2018] http://www.elfinanciero.com.mx/tech/facebook-se-hunde-por-el-robo-de-datos

EL UNIVERSAL. (2018). *Facebook amplía a 87 millones el número de usuarios afectados por robo de datos.* Fecha de publicación: 4 de abril de 2018. [Consultado: 16 de febrero 2019] [En línea] http://www.eluniversal.com.mx/mundo/facebook-amplia-87-millones-el-numero-de-usuarios-afectados-por-robo-de-datos

ERNST & YOUNG GLOBAL. (2015). *Crear confianza en el mundo digital. Encuesta Global sobre Seguridad de la Información de EY de 2015.* 18° edición, 2015. [Consultado: 18 de enero 2019] [En línea] https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2015/%24FILE/ey-encuesta-global-seguridad-informacion-2015.pdf

EXPANSIÓN. (2014). Muerte de MT.GOX, ¿El fin del Bitcóin?, *Sección: economía.* Fecha de publicación: 26 de febrero de 2014. [Consultado: 22 de marzo 2019] [En línea] https://expansion.mx/economia/2014/02/26/muerte-de-mtgox-el-fin-del-bitcoin

GONZALEZ Alcalá, A. II y DAVID GÓMEZ, D. (2015). *Guía práctica InnoViTech: Vigilancia Tecnológica para la Innovación.* Servicio Nacional de Aprendizaje, SENA: Rionegro-Antioquia, 2015. 62 p. [Consultado: 9 de marzo 2019] [En línea] https://es.slideshare.net/nestorg10/gua-prctica-innovitech-2015

GONZÁLEZ BRITO, H. R., ANGLADA MARTÍNEZ, R. A. y GAINZA REYES, D. (2018) "El papel de la vigilancia tecnológica en la disminución de Incidentes de ciberseguridad en aplicaciones web." *Universidad de las Ciencias Informáticas. Habana, Cuba*. [Consultado: 13 de febrero de 2019 [En línea] https://www.researchgate.net/publication/317175399_EL_PAPEL_DE_LA_VIGILANCIA_TECNOLOGICA_EN_LA_DISMINUCION_DE_INCIDENTES_DE_CIBERSEGURIDAD_EN_APLICACIONES_WEB]

HUFFPOST. (2018). *El caso Cambridge Analytica y el robo de datos de FB en México, ¿Cómo me protejo?* [Negoción] Fecha de publicación: 20 de marzo de 2018. Fecha de actualización: 21 de marzo de 2018. [Consultado: 11 de febrero 2019] [En línea] https://www.huffingtonpost.com.mx/2018/03/20/el-caso-cambridge-analytica-y-el-robo-datos-de-fb-en-mexico-como-me-protejo_a_23390721/

LA JORNADA. (2017). *México ocupa el octavo lugar de robo de identidad en todo el mundo con más de 50 mil denuncias.* Fecha de publicación: 16 de diciembre de 2017. [Consultado 5 de febrero 2019] [En línea] http://www.lja.mx/2017/12/mexico-ocupa-octavo-lugar-robo-identidad-en-mundo-50-mil-denuncias/

LAGUNES Soto, V. (2018). *Ciberseguridad.* Jefe de la Unidad de Innovación y estrategia tecnológica de la Presidencia de la Republica. Ponencia Magistral (Foro de ciberseguridad). [Consultado: 15 de marzo 2019] [En línea] https://www.gob.mx/cnbv/videos/foro-ciberseguridad-ponencia-magistral

LESWING, K. (2018). *Un ciberataque masivo noqueó a los principales sitios web en Internet.* [Consultado: 5 de mayo 2018] [En línea] https://www.businessinsider.com/amazon-spotify-twitter-github-and-etsy-down-in-apparent-dns-attack-2016-10&prev=search

MENDOZA, M. A. Welivesecurity. (2015). *¿Ciberseguridad o seguridad de la información? Aclarando la diferencia.* Fecha de publicación: 16 de junio de 2015. [Consultado: 25 de enero 2019] [En línea] https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

MÉXICO. Constitución Política de los Estados Unidos Mexicanos. DOF. 15 de septiembre de 2017.

MÉXICO. Ley General de Archivos. DOF. 15 de junio de 2019.

MÉXICO. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. DOF. 26 de enero de 2017.

RAMIREZ ACEVES, M.C.; SANCHEZ ESPINOZA, A.; BIRRICHAGA GARDIDA, D. y BELTRAN CABRERA, L. “El devenir histórico de la cultura archivística en México.” *Inf. cult. soc.* 2011, n.24 [citado 2018-06-07], pp.39-68. [Consultado: 15 de febrero 2019] [En línea] http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1851-17402011000100003

VOUTSSÁS M., J. (2010). “Preservación Documental Digital y Seguridad Informática.” *Investigación Bibliotecológica.* Centro Universitario de Investigaciones Bibliotecológicas, UNAM. (Vol. 24, no. 49.) Citado en: Archivos Electrónicos Textos y Contextos. [Consultado: 19 de marzo 2019] [En línea] http://www.interpares.org/display_file.cfm?doc=ip3_mexico_dissemination_bc_voutsass_archivos-electr%C3%B3nicos_2011.pdf