REVISTA DEL ARCHIVO NACIONAL DE COSTA RICA

ISSN 2215-5600
Vol. 86, 2022: e578
Del 1 de enero al 31 de diciembre 2022
www.archivonacional.go.cr/RAN



Artículo arbitrado, sección ARCHIVÍSTICA

Ciberseguridad, archivos y el derecho de intimidad: confluencia e importancia desde el campo de acción de la archivística

Cybersecurity, archives and right to privacy: confluence and importance from the archivist action field

Valeria Espinoza González

Bachiller en Archivística por la Universidad de Costa Rica. valeeg_95@hotmail.com | COSTA RICA.

Fecha de recepción: 29/06/2022
Fecha de aprobación: 11/10/2022

Alejandro Salazar Zúñiga

Bachiller en Archivística por la Universidad de Costa Rica. alesazu24@gmail.com | COSTA RICA.

RESUMEN. Este artículo trata sobre la importancia del quehacer archivístico en el campo de la ciberseguridad como un elemento clave y estratégico; debido a que la Archivística permite tener un amplio panorama desde la perspectiva de la gestión documental y las necesidades de protección y seguridad que debe tener la información y los documentos de archivo. Asimismo, desde una perspectiva de protección del derecho a la intimidad de las

personas, la Archivística plantea soluciones con el fin de mantener segura la información íntima de las personas, y proporcionar acceso solo a aquella información que no violente de ninguna manera el derecho a la intimidad. Esto convierte a la profesión en uno de los ejes fundamentales sobre los cuales debe girar la protección de la información, no solo en formato físico sino también electrónico. Finalmente, se establece la diferencia entre el rol que cumple la persona archivista y el rol que cumple la persona profesional en informática con respecto al tema de la ciberseguridad, lo cual requiere de un compromiso interdisciplinario para ser llevado a cabo de la mejor manera.

PALABRAS CLAVE. Ciberseguridad; derecho a la intimidad; archivística; información; roles.

ABSTRACT. *This article is about the importance of the archivist duty in the cybersecurity field, seen as a key and strategic element; due to the archivist being able to have a wide panorama from the perspective of records management and the needs related to the protection and security that the information must have.*

Likewise, from a human right to privacy perspective, archiving proposes solutions in order to keep information accessible to citizens, this being a guarantee of the fulfillment of rights.

This makes the archivist profession one of the fundamental axes on which the protection of information must revolve, not only in physical format but also digital format.

Finally, the difference between the role played by the archivist and the role played by the IT Engineer is established for the issue of cybersecurity, which requires an interdisciplinary commitment to be carried out in the best way.

KEYWORDS. *Cybersecurity; right to privacy; archivist; information; roles.*

1. INTRODUCCIÓN

El aumento paulatino de herramientas tecnológicas y el acceso cada vez más generalizado a información disponible en medios digitales han representado nuevos desafíos para las personas profesionales en la gestión de la información; así como para las personas creadoras y usuarias de cada una de las plataformas electrónicas existentes. Prueba de ello son los recientes ataques cibernéticos sufridos por varias instituciones públicas costarricenses, que han provocado la vulnerabilidad de datos y la pérdida del acceso a la información pública. Esto ha generado daños significativos en materia fiscal, sanitaria y de prestación de servicios en general.

Desde esta óptica surge el debate sobre si la Archivística debe intervenir en materia de ciberseguridad o si, por el contrario, este es un tema concerniente únicamente de las personas profesionales en informática. Es por ello que la intención del presente estudio es analizar esta conexión interdisciplinaria entre el papel que cumple la persona archivista dentro de las organizaciones, en conjunto con el papel que desempeñan el resto de los profesionales de las tecnologías de la información y comunicación. De tal forma que, la presente investigación pretende mostrar desde una perspectiva analítica la teoría y conceptos que permitan comprender esta relación, y delimitar los roles que podría cumplir la persona archivista para aportar en materia de seguridad de la información en ambientes tecnológicos, como lo son los Sistemas de Gestión de Documentos Electrónicos de Archivo, y cómo esto va ligado con el tema de la protección del derecho a la intimidad, al proteger los activos de información que contengan datos sensibles o información de acceso restringido.

1.1. Justificación

El tema que se desarrolla en el presente artículo se considera de suma importancia para la profesión Archivística, ya que en el contexto actual, en el que se avanza cada vez más rápido en temas tecnológicos, es indispensable que el gremio de archivistas se integre a la toma de decisiones en lo concerniente a la gestión de la información, no solo en soporte papel, sino también en soportes electrónicos, ya que hoy por hoy los archivos no se constituyen solamente como un espacio físico dentro de una institución, si no que ahora existe la posibilidad de gestionar documentos e información en medios digitales, los cuales requieren del mismo tratamiento archivístico que los documentos en soporte papel.

Es por ello que existe una clara necesidad de que se indague desde el punto de vista archivístico, sobre los diferentes ámbitos de acción en materia tecnológica, en los cuales las personas profesionales en Archivística pueden ser partícipes en la toma de decisiones, debido a su clara competencia en cuanto a los requerimientos sobre gestión de la información, seguridad, acceso, por mencionar algunos, y en este caso se muestra que la ciberseguridad en definitiva es un área en la cual la Archivística tiene conocimiento que aportar para la protección de la información que se gestiona a lo interno de las organizaciones.

1.2. Delimitación espaciotemporal

El desarrollo de la investigación se delimita en un contexto histórico muy específico: la ola de ataques cibernéticos recibidos por diversas instituciones públicas costarricenses en el año 2022. Y es que; aunque no es la primera vez que los sitios web del sector público costarricense se ven vulnerados por ciberdelincuentes; el ataque del ransomware "Conti" ha marcado un hito en nuestro país. El artículo fue elaborado entre los meses de abril a octubre del año 2022.

1.3. Problema

En relación con el problema de investigación, se debe tomar en cuenta que la seguridad de la información constituye uno de los pilares fundamentales de la transparencia y la prestación de servicios que ofrecen las instituciones públicas y privadas. Desde esta perspectiva surge la inquietud sobre cómo se está garantizando esa seguridad de la información, y las razones por las que las personas profesionales en Archivística, como gestores de la información, no están participando en propiciar su resguardo a través de mecanismos electrónicos. La información insegura acrecienta la posibilidad de violentar el derecho a la intimidad, debido a los parámetros aplicados en cuanto al acceso a la información, y la Archivística parece estar contribuyendo poco para solventar este problema.

1.4. Objetivos

1.4.1. Objetivo general

Analizar la relación entre el campo de acción de la Archivística, y cómo esta puede ser parte de la toma de decisiones en materia de ciberseguridad, con el fin de garantizar la protección de los datos e información que se custodia y gestiona en entidades tanto públicas como privadas, para garantizar la protección del derecho a la intimidad por medio de la protección de la información y documentos electrónicos de archivo.

1.4.2. Objetivos específicos

- Identificar la relación existente entre la Archivística y la ciberseguridad.
- Establecer la relación entre la Archivística con respecto a la protección del derecho a la intimidad.
- Determinar la forma en la cual la ciberseguridad incide en la protección del derecho a la intimidad, por medio de la protección de la información desde el punto de vista archivístico.

2. TIPO Y ENFOQUE DE INVESTIGACIÓN

Al tratarse de una temática incipiente, la investigación realizada corresponde al tipo de investigación indagatoria, ya que se basa en la búsqueda y análisis de fuentes secundarias que permita obtener un panorama sobre la situación actual con respecto al papel que cumple la Archivística dentro del ámbito tecnológico en el tema de la ciberseguridad, entendida como un elemento clave para proteger los activos de información de los Sistemas de Gestión de Documentos Electrónicos de Archivo, y su relación directa con la protección de derechos, como lo es el derecho a la intimidad.

Por otro lado, la investigación responde a un enfoque cualitativo, esto debido a que los fenómenos a investigar (ciberseguridad y Archivística) son amplios, por lo que resulta vital contextualizar ambos términos desde el inicio y durante el transcurso de la investigación. Además, se analizan realidades subjetivas, pues el artículo reúne elementos que tienen una incidencia en fenómenos sociales que abarcan aspectos como la transparencia, el

acceso a la información y la seguridad de los datos. El resultado esperado contemplaría una riqueza interpretativa importante, pues se pretende que las conclusiones a las que se llegue constituyan un insumo para la implementación y el desarrollo de estudios similares en las instituciones públicas y privadas.

2.1. Población o muestra

Cabe aclarar que en esta investigación no fue necesario utilizar ningún tipo de población o muestra, ya que, como se ha mencionado, la investigación requirió únicamente de la recopilación y análisis de fuentes de información que proporcionan las conceptualizaciones necesarias para establecer la relación entre la Archivística, la ciberseguridad y el derecho a la intimidad.

2.2. Fuentes de información

Para el desarrollo de esta investigación se utilizó como principal insumo el análisis de fuentes bibliográficas recopiladas a través de servicios en línea y bases de datos web. Tomando en cuenta la recolección de información de fuentes secundarias tales como revistas, trabajos finales de graduación, libros, entre otras.

3. RELACIÓN ENTRE ARCHIVÍSTICA Y CIBERSEGURIDAD

En primera instancia, es importante comprender en qué consiste el concepto de ciberseguridad. La transnacional CISCO (2021) la define en su página web como la "práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; extorsionar a las personas usuarias o interrumpir la continuidad del negocio". Desde esta primera definición se puede vislumbrar un enlace directo con la Archivística, pues el acceso, la modificación y la destrucción de información se debería realizar a través de criterios técnicos archivísticos, que evidentemente se violentan a través de los ciberataques.

Se debe recordar que la Archivística cuenta con diferentes fases, en las cuales se debe realizar, en primera instancia, la identificación de los tipos documentales o de la información con la

cual se está trabajando, posteriormente, tales documentos de archivo o información debe ser clasificada bajo diferentes modelos que permitan hacer posible su recuperación teniendo claridad del expediente en el cual se encuentra contenida. Una vez que la identificación y la clasificación se ha realizado, se deben aplicar otros procedimientos como lo es la creación de tablas de acceso en las que se defina quiénes tendrán acceso a los diferentes expedientes o determinada información, tomando en consideración la clasificación previa, ya que, si se ha determinado que cierto expediente posee información confidencial, es evidente que su acceso será restringido, o por el contrario, pueden existir expedientes de acceso irrestricto.

Asimismo, cuando se trata del proceso de eliminación, se debe elaborar una tabla de plazos en la cual se establezca el periodo en el cual se debe conservar cada expediente dependiendo del tipo de información que posea, por lo tanto, existirá información que deba ser conservada durante diez años o más, o incluso puede haber información que se conserve únicamente por un periodo de dos años. De tal forma que, es necesario aplicar los procesos archivísticos para garantizar la seguridad de aquella información que inicialmente se haya identificado como vital para una organización, y también para toda aquella información que se haya establecido como confidencial, por ende, los mismos procesos deben ser aplicados a sistemas de gestión de documentos electrónicos, ya que indistintamente del soporte en el cual se encuentren los documentos de archivo, es fundamental identificar y clasificar la información para posteriormente aplicar las medidas de seguridad necesarias de acuerdo al nivel de relevancia que posea para la organización.

Por otro lado, otra definición que reafirma la relación directa entre la Archivística y la ciberseguridad es la que ofrece Leiva (2015), quien indica que la ciberseguridad se refiere a "métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio". (p.162). Estos elementos mencionados por el autor, responden a varios de los aspectos esenciales en el quehacer archivístico, y nos obliga como profesionales de la información a involucrarnos directamente en el tema, ya que, como es bien sabido, la Archivística es una profesión que se encarga de garantizar la confidencialidad de los documentos de archivo, esto por medio del conocimiento y aplicación de la normativa vigente en materia de gestión de la información, y también por medio de la creación de las tablas de acceso; además, la Archivística debe procurar la integridad de los documentos, evitando modificaciones o alteraciones de la información contenida en ellos, ya que para la Archivística es vital mantener los documentos

íntegros debido a su valor probatorio y legal, además de la disponibilidad de la información, aspecto para el cual se crean los cuadros de clasificación que permitan su rápida localización, esto tanto en un archivo con documentos en soporte papel, como en un sistema de gestión de documentos electrónicos.

Por tales motivos, no se debe dejar de lado que la Archivística posee una relación directa con la ciberseguridad, en tanto que ambas disciplinas deben realizar esfuerzos para procurar la confidencialidad, integridad, y disponibilidad de la información. Asimismo, la persona profesional en Archivística funge también como protectora de la información que custodia; por este motivo, la confidencialidad adquiere un papel fundamental en los sistemas de gestión de documentos, entiéndase este como un sistema que puede ser aplicable tanto a documentos en soporte papel como en soporte electrónico, y para este segundo caso se hace referencia a sistemas de gestión de documentos electrónicos. A la luz de estos sistemas es importante conocer el término del ciber espionaje, que según Maroto (2009) consiste en "realizar reconocimientos de los sistemas de información de gobiernos, universidades y compañías privadas, identificando los objetivos clave, buscando vulnerabilidades e introduciendo «puertas traseras» para su empleo en tiempos de crisis o confrontación". (p.55).

Como se puede interpretar de la definición anterior, existen técnicas variadas que se utilizan para violentar la información a través de los sistemas informáticos, por lo que la ciberseguridad adquiere un papel preponderante para salvaguardar la información de gran valor contenida en estos sistemas, así como los derechos de las personas que poseen relación directa con tal información. Ahora bien, el Comité Interministerial sobre ciberseguridad (2017) es una organización encargada de elaborar la Política Nacional de Ciberseguridad de Chile. Este Comité señala que la ciberseguridad es importante para:

a. Resguardar la seguridad de las personas en el ciberespacio.
b. Proteger la seguridad de un país.
c. Promover la colaboración y coordinación entre instituciones.
d. Gestionar los riesgos del ciberespacio.

A partir de lo señalado por las fuentes citadas anteriormente, podría concluirse que es innegable la injerencia de la persona archivista en aspectos de seguridad de la información, y que es un deber profesional que se involucre en esta área. Justamente, Moreno (2017) señala que "los recientes ciberataques a nivel mundial han dado lugar a verdaderas crisis y han puesto de manifiesto que la ciberseguridad requiere del compromiso y colaboración de todos aquellos organismos y personas que utilizan la tecnología". (p.54). Es por esto que la Archivística es una profesión que puede tomar mucha fuerza, debido a su relevancia a nivel institucional y gubernamental, gracias a los aportes que puede proveer en materia de gestión de documentos sobre todo en soportes electrónicos, lo cual es un ámbito poco explorado en la actualidad y razón por la cual diversas instituciones públicas del país se han visto afectadas tanto en su quehacer cotidiano como en los servicios que brindan a la ciudadanía por los ciberataques recibidos, debido a la deficiente gestión de los documentos electrónicos de archivo que carecían de la seguridad adecuada en los sistemas de información utilizados.

Además, parte del trabajo que debe realizar una persona profesional en Archivística, es gestionar el riesgo que supone la pérdida, eliminación, robo, entre otros, de los documentos de archivo e información que custodia. Es por esto que no se trata solamente de la gestión de los documentos de archivo entendida como la ordenación y clasificación de los documentos, si no que va más allá, ya que a través del análisis de identificación que se realiza para determinar las funciones y procesos de una organización, también se logra identificar los tipos documentales que se producen a través de tales procesos y funciones. Posterior a esto, se determina su respectiva clasificación, como ya se ha mencionado, para ordenarlo adecuadamente en expedientes ya sean físicos o electrónicos. Pero esta labor es mucho más valiosa de lo que a simple vista puede parecer, ya que a raíz de tener identificados los procesos organizacionales y los documentos que surgen de estos, se puede realizar un análisis de riesgos que permita identificar los procesos sustantivos de la organización y por ende los documentos vitales que permitirían la continuidad del negocio ante cualquier eventualidad, incluyendo un ciberataque, lo cual es sumamente valioso para cualquier organización, ya que teniendo claro este panorama se pueden tomar las medidas necesarias para mitigar cualquier riesgo que comprometa la continuidad de las actividades y los servicios que se le brinda a la ciudadanía.

Por otro lado, Galán y Galán (2016) brindan un panorama en relación con el deber de participación de las personas profesionales en Archivística en materia de ciberseguridad,

aclarando la relación entre ambas áreas del saber al referirse al concepto de "digitalización de la sociedad" de la siguiente manera:

> La llamada "digitalización de la sociedad" exige garantizar que las herramientas tecnológicas utilizadas tienen la capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas prestan o hacen accesibles. (p. 294).

En relación con la cita anterior, se destaca la oportunidad con la que cuentan las personas profesionales en Archivística a través del levantamiento de requisitos para sistemas de gestión de documentos electrónicos (SGDE), esto para garantizar que la información contenida se encuentre disponible, auténtica, íntegra y confiable. Este es un aspecto que en definitiva se debe trabajar, ya que en el mercado actualmente existen múltiples empresas que brindan soluciones informáticas de sistemas de gestión de documentos electrónicos, pero que en realidad estas soluciones no pueden ser aplicables a cualquier organización, ya que cada organización es diferente y los sistemas que se implementen deben ser adaptables a la realidad y las necesidades de cada una. Es por esto que las personas archivistas deben intervenir en un trabajo interdisciplinario al momento de llevar a cabo proyectos de desarrollo e implementación de sistemas a nivel institucional, ya que estos son los profesionales que realmente conocen o saben identificar las necesidades de gestión de la información que requiere la organización, así como el nivel de seguridad con el que deben contar determinadas series documentales. Estas son competencias específicas de estos profesionales, y no deben ser delegadas a profesionales de otras áreas.

Ciertamente, las personas profesionales en informática deben ejecutar las acciones correspondientes para que los sistemas organizacionales posean la máxima seguridad necesaria para evitar ciberataques o pérdida de información en general, no obstante, las personas profesionales en Archivística deben plantear los requisitos iniciales del sistema, para que este gestione adecuadamente los documentos electrónicos, procurando su correcta clasificación dentro del sistema, la generación de los metadatos necesarios para su recuperación y para obtener la trazabilidad del documento, logrando identificar quién tuvo acceso a este, si fue modificado o no, la fecha de creación del documento, quién lo creó, a

cuáles unidades tuvo alcance el documento, entre muchos otros elementos indispensables para tener un control adecuado de los documentos electrónicos y garantizar su autenticidad, integridad y disponibilidad.

Sin embargo, el rol de archivista no se limita únicamente al levantamiento de requisitos para sistemas, sino que abarca también otras acciones que permiten a las instituciones fiscalizar de una mejor manera el trasiego de la información, así como la seguridad de los datos que se custodian. En relación con lo anterior, Fonseca y Juárez (2019) señalan aspectos que se pueden implementar desde los archivos para la protección de datos personales en relación con la ciberseguridad y la vigilancia tecnológica:

- 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 quién 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 disponibles 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. 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).
- Considerar los 6 puntos de la cadena de preservación digital que señala Voutssás (2010), en la cual 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; así se mantendrá un control de los documentos, permitiendo saber quién es el responsable de cada uno de ellos, así como quién y cuándo los consultó (pp. 238-240).

Como se puede observar, es amplio el panorama para que el gremio de archivistas pueda participar en materia de ciberseguridad. Además, en la actualidad existen múltiples áreas en

las cuales los profesionales en Archivística se pueden desempeñar, sobre todo en el ámbito tecnológico, como ya se ha mencionado en materia de ciberseguridad, pero también en el planteamiento de requisitos para el desarrollo de sistemas de gestión de documentos electrónicos, gestión del riesgo y seguridad de la información vital para la organización, entre otros. Es cuestión de tomar acción e incentivar a este grupo de profesionales en que es posible adaptarse a los nuevos retos y cambios tecnológicos. Citando a Fonseca y Juárez (2019):

> 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 físicamente, sino también mediante el uso de la tecnología. La labor de los archivistas retoma cada vez mayor importancia, 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. (p. 242).

4. RELACIÓN ENTRE ARCHIVÍSTICA Y EL DERECHO A LA INTIMIDAD

El fin principal de la Archivística es hacer accesible la información a lo largo del tiempo, tanto para la ciudadanía como a las diferentes personas involucradas en los procesos o funciones organizacionales de las instituciones u organizaciones. Por eso es indispensable la labor archivística con el objetivo de mantener la información a la mano, organizada y accesible de manera rápida y eficaz para todas las personas. No obstante, así como la Archivística se encarga de hacer accesible la información, también debe conocer muy bien la normativa que regula el derecho a la intimidad, y que existe cierto tipo de información o documentos de archivo que no pueden ser facilitados debido al componente de confidencialidad que supone determinada información de carácter personal.

Además de lo anterior, como ya se ha mencionado líneas arriba, la Archivística se encarga de la ardua y delicada tarea de identificar el tipo de información que se gestiona, clasificando

y valorando de acuerdo con criterios técnicos y legales que le permitan establecer si determinada información es de carácter confidencial, de acceso restringido, de acceso irrestricto, datos personales, entre otros. Todo esto es fundamental para garantizar la adecuada gestión de los datos, respetando los criterios legales que se establecen sobre el manejo de la información, sobre todo si es confidencial o íntima, por lo que no debe ser revelada en ninguna circunstancia a terceros.

Bajo esta misma línea y relacionando el quehacer archivístico con la protección de los Derechos Humanos en materia de información, según el texto Derechos Humanos de la Unión Interparlamentaria (2016) se definen los derechos humanos de la siguiente manera:

> Los derechos humanos son derechos inherentes a todas las personas. Definen las relaciones entre los individuos y las estructuras de poder, especialmente el Estado. Delimitan el poder del Estado y, al mismo tiempo, exigen que el Estado adopte medidas positivas que garanticen condiciones en las que todas las personas puedan disfrutar de sus derechos humanos. (pág. 19).

De acuerdo con la cita anterior, se puede establecer la relación entre los individuos, entendidos estos como la sociedad civil, y las estructuras de poder, que se refieren a los distintos organismos que componen el Estado. Ahora bien, sobre esta misma relación se establece que el Estado es quien debe garantizar que los derechos humanos se cumplan para todas las personas sin distinción alguna. Por eso, desde los distintos organismos estatales se deben aplicar las medidas necesarias para que la información que se gestiona tanto de manera electrónica como física sea identificada, clasificada, evaluada y conservada. Todo esto de acuerdo con el análisis y criterios archivísticos establecidos para tal fin, con el objetivo de garantizar que la información sensible, confidencial y de acceso restringido no sea accesada fácilmente por terceras personas, y que esto conlleve a la violación del derecho a la intimidad de las personas que posean relación directa con la información. Otra definición de derechos humanos es la que nos ofrece Reyes Prado (s.f.) cuando cita a Eusebio Fernández (1984), quien menciona que:

> los derechos humanos tienen su fundamento antropológico en la idea de necesidades humanas, que se tratan de satisfacer con el reconocimiento, ejercicio y protección de los derechos, lo cual requiere la existencia de medios suficientes y posibilidades reales para la satisfacción de tales necesidades, sin lo que es imposible hablar

> de derechos, que implican la imposición sobre otros de los correlativos deberes. Este autor sostiene que, paralelamente a la posesión de derechos fundamentales, existen deberes y obligaciones fundamentales; nexo que no debe negarse, pues poseer un derecho en el sentido jurídico del término equivale a la imposición por parte del ordenamiento jurídico de un deber jurídico correlativo y complementario a otra persona o a la misma. Indica que, los derechos son lógica y axiológicamente anteriores a los deberes, pues determinan una necesidad incondicional, así como las posibilidades reales de satisfacerla, se puede establecer el deber correlativo, por lo que los derechos justifican los deberes. (pp. 7-8)

De acuerdo con lo anterior, se refuerza la idea de que el Estado es quien debe garantizar la protección de los derechos humanos de la población, para lo cual es indispensable que se articulen los mecanismos necesarios. Es desde la parte legal, tanto a nivel país como a lo interno de cada institución, donde se deben dictar las diferentes políticas, directrices o insumos que establezcan los criterios a cumplir en materia de gestión documental, para que esto garantice la adecuada gestión de la información. Lo anterior con el objetivo de cumplir satisfactoriamente la necesidad de protección y seguridad de la información tanto a las personas como a las organizaciones que tienen la obligación de cumplir en ese aspecto.

Ahora bien, en la legislación costarricense sí existe una normativa que regula el tema del tratamiento de la información, con un enfoque ligado a la protección del derecho a la intimidad en este sentido. Esto por medio de la Ley No. 8968 sobre la Protección de la Persona frente al tratamiento de sus datos personales. De tal forma que el artículo 10 de la Ley No. 8968 menciona lo siguiente:

> Artículo 10. - Seguridad de los datos: El responsable de las bases de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley.
>
> Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada.
>
> No se registrarán datos personales en bases de datos que no reúnan las condiciones

> que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas.
>
> Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos.

Además, el artículo 12 de esta misma ley, que se refiere a los protocolos de actuación, establece lo siguiente:

> Artículo 12.- Protocolos de actuación: Las personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, el almacenamiento y el uso de datos personales, podrán emitir un protocolo de actuación en el cual establecerán los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales, de conformidad con las reglas previstas en esta ley.
>
> Para que sean válidos, los protocolos de actuación deberán ser inscritos, así como sus posteriores modificaciones, ante la Prodhab. La Prodhab podrá verificar, en cualquier momento, que la base de datos esté cumpliendo cabalmente con los términos de su protocolo.
>
> La manipulación de datos con base en un protocolo de actuación inscrito ante la Prodhab hará presumir, "iuris tantum", el cumplimiento de las disposiciones contenidas en esta ley, para los efectos de autorizar la cesión de los datos contenidos en una base.

De tal forma que en Costa Rica se puede evidenciar que existe legislación que regula el proceso del manejo de la información; además se señala que existe otra instancia como la Prodhab, la cual se encarga de verificar que las bases de datos cumplan con los respectivos protocolos. Por lo tanto, existe todo un entramado que regula el tema de la gestión de la información y los datos, por lo que se esperaría que las diferentes instituciones que componen el aparato estatal realmente garanticen la seguridad de la información y su correcta gestión.

Además, la Constitución Política de la República de Costa Rica, en su título IV, denominado *Derechos y Garantías Individuales, Capítulo Único,* tiene un artículo relacionado con los derechos que posee toda persona costarricense en relación con la información y comunicaciones, las

cuales son de carácter privado debido al derecho de intimidad de la persona. A continuación, se cita el artículo 24 de la *Constitución Política*:

> ARTÍCULO 24.- Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones.
>
> Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.
>
> Igualmente, la ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo. Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán ser razonadas y podrán ejecutarse de inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial.
>
> La ley fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los libros de contabilidad y sus anexos para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos.
>
> Una ley especial, aprobada por dos tercios del total de los Diputados, determinará cuáles otros órganos de la Administración Pública podrán revisar los documentos que esa ley señale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa revisión.
>
> No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación.

Como se puede observar, constitucionalmente se encuentra establecido el derecho a la intimidad, a la libertad y al secreto de las comunicaciones, y el mismo artículo menciona que se debe garantizar ese derecho. Por lo tanto, es crucial que cada institución establezca y aplique los protocolos necesarios para garantizar la seguridad de la información por dos motivos: el primero es que se garantice la protección de los derechos humanos y el segundo es que se cumpla lo que constitucional y legalmente se ha establecido. De lo contrario se estaría violando el marco jurídico y además violentando uno de los derechos inherentes a todo ser humano: su derecho de intimidad y protección de la información de carácter personal.

Por eso la Archivística juega un papel fundamental en la creación de políticas o protocolos que permitan establecer los lineamientos y requerimientos necesarios para garantizar la adecuada gestión y protección de la información, ya que durante mucho tiempo la Archivística se ha encargado de emitir lineamientos en materia de gestión de documentos físicos. Sin embargo, en la actualidad, con el uso de la tecnología, ha surgido una nueva variable: el documento electrónico, y con ello la adaptación de la archivística con respecto a la gestión de los documentos electrónicos, los cuales requieren del mismo tratamiento archivístico, pero en entornos digitales.

5. ROLES ENTRE INFORMÁTICOS Y ARCHIVISTAS, ¿DÓNDE CONVERGEN?

Actualmente existe una confusión con respecto a la forma en la cual se gestiona la información en entornos digitales, esto debido a que el quehacer de las personas profesionales en informática ha cobrado gran relevancia con respecto a la forma en la cual se gestionan las bases de datos, ya que se considera que son estas personas quienes tienen el conocimiento sobre cómo se debe almacenar y gestionar la información en estos medios tecnológicos. Si bien es cierto realizan las programaciones necesarias para crear una base de datos con todas las características pertinentes de acuerdo a los requerimientos establecidos y solicitados por las diferentes instancias que plantean una propuesta de proyecto de implementación de una base de datos o sistema de gestión de documentos electrónicos, esto no quiere decir que dentro de la formación académica de este profesional se incluyan los conocimientos necesarios para saber gestionar la información.

Por lo anterior, resulta fundamental la intervención de las personas profesionales en Archivística, quienes sí tienen la formación académica y las competencias necesarias para saber gestionar la información que se encuentra en medios digitales, ya que los documentos electrónicos requieren del mismo tratamiento archivístico que los documentos en soporte papel. Por lo tanto, se debe diferenciar muy bien que la persona profesional en informática solamente crea la base de datos o el sistema de gestión de documentos electrónicos y le da soporte para solucionar fallas o implementar nuevos requerimientos; y por otro lado, la persona profesional en Archivística indica las pautas y requerimientos necesarios con los que debe contar el sistema para que cumpla adecuadamente con los procesos de creación, distribución, firma, accesos, preservación de la información y muchos otros elementos indispensables.

De tal forma que las organizaciones no deberían menospreciar la labor Archivística en el sentido de que es una profesión clave en la correcta toma de decisiones para mejorar el proceso de gestión de documentos en los diferentes sistemas que se manejan a nivel institucional. Además, para la elaboración de políticas que permitan establecer los criterios necesarios para garantizar la seguridad, trazabilidad, recuperación y acceso de la información, tomando en cuenta criterios archivísticos y de valoración documental.

De ahí la complementariedad de la Archivística con el tema de la ciberseguridad, ya que desde el punto de vista de la disciplina resulta clave que se identifiquen las series documentales que se gestionan en los medios electrónicos, para poder determinar su valor dentro de la organización. De esta forma se pueden aplicar las medidas de seguridad correspondientes de acuerdo con las series documentales que son de mayor importancia para la continuidad del negocio, así como la información relacionada con datos sensibles o de acceso restringido, con el fin de salvaguardar la información de la mejor manera posible.

6. RELACIÓN ENTRE LA APLICACIÓN DE LA CIBERSEGURIDAD EN LA ARCHIVÍSTICA, Y CÓMO ESTA INCIDE EN LA PROTECCIÓN DEL DERECHO A LA INTIMIDAD

De acuerdo con los puntos señalados anteriormente, se puede evidenciar la importancia del papel que juega la Archivística con respecto al tema de la ciberseguridad en las organizaciones, ya que desde este punto de vista existen una serie de elementos a tomar en cuenta para poder clasificar la información y así determinar cuántos esfuerzos o recursos deben destinarse en la protección de determinadas series documentales.

Aunado a esto y a su relación con los derechos humanos, según Serrano & Vázquez (2011): "se establece como punto de partida que los derechos humanos son exigencias éticas justificadas, especialmente importantes, que deben ser protegidas eficazmente a través del aparato jurídico" (pág. 13). Desde la perspectiva archivística, y desde la ética de trabajo en esta rama de estudio, es fundamental garantizar que la información sea resguardada para poder acceder a ella en el largo plazo. Por eso se realizan múltiples esfuerzos por mantener la información disponible para la ciudadanía, pero al mismo tiempo se debe mantener una ética en cuanto a los documentos que sean de carácter confidencial o de acceso restringido por los diferentes motivos legales que justifiquen dicha clasificación; y de acuerdo con ello, deben existir mecanismos que garanticen que ninguna persona no autorizada será capaz de acceder a la información. Esto es parte de garantizar al mismo tiempo la protección de los derechos individuales al proteger la información que contenga datos sensibles o información íntima. Al respecto, el artículo 3 de la Ley n.º 8968 se refiere a las siguientes definiciones:

> Artículo 3.- Definiciones
>
> a) Base de datos: cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales que sean objeto de tratamiento o procesamiento, automatizado o manuales, cualquiera que sea la modalidad de su elaboración, organización o acceso.
>
> b) Datos personales: cualquier dato relativo a una persona física identificada o identificable.

> c) Datos personales de acceso irrestricto: los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.
>
> d) Datos personales de acceso restringido: los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.
>
> e) Datos sensibles: información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.
>
> i) Tratamiento de datos personales: cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.

En este sentido, es necesario rescatar que la aplicación del tratamiento archivístico a los activos de información debe ser acorde con el acatamiento de la legislación en materia de gestión de documentos y tratamiento de datos personales de la sociedad civil. Además, la ciberseguridad debe ir en esta misma línea, abocada al cumplimiento en materia legal que garantice la protección de los datos sensibles de las personas. Por esto no es adecuado referirse a la ciberseguridad como algo que atañe únicamente a las personas profesionales en informática o a los departamentos de tecnologías de información, si no que requiere de un trabajo multidisciplinar que permita aplicar los conocimientos técnicos tecnológicos; también los conocimientos en materia archivística y de gestión de la información, la cual engloba aspectos tecnológicos, legales, técnicos, archivísticos, entre otros.

Asimismo, en la Carta de los Derechos Fundamentales de la Unión Europea existen varios artículos relacionados con los derechos atinentes a la información, datos, comunicaciones y a la privacidad de todo ser humano en relación con estos elementos. Dichos artículos se citan a continuación:

> ARTÍCULO 7.- Respeto de la vida privada y familiar: Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.
>
> ARTÍCULO 8.- Protección de datos de carácter personal:
>
> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
>
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
>
> 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Se considera relevante para el tema en estudio indagar sobre las distintas perspectivas en el ámbito internacional con relación al derecho de intimidad y el manejo/acceso de la información, ya que es importante analizar que desde distintas latitudes este tipo de derechos se mantienen similares. De tal forma que, no es cuestión de que a nivel país se definan cuáles son los derechos que se deben proteger en relación con el manejo de la información mediante normativa y legislación nacional, sino que estos derechos son inherentes a todo ser humano desde cualquier parte del mundo, como lo es el derecho a la protección de datos de carácter personal, privacidad de las comunicaciones, solo por mencionar algunos ejemplos en materia de información.

Asimismo, los sistemas de gestión de documentos electrónicos que se desarrollen e implementen en las organizaciones tanto gubernamentales como no gubernamentales, deberían contar con mecanismos de ciberseguridad adecuados para proteger la información ante ataques cibernéticos que puedan violentar el derecho a la intimidad de las personas. Para eso, la Archivística juega un papel fundamental, como se ha señalado con anterioridad al relacionar la ciberseguridad con la Archivística y las fases del tratamiento archivístico que son indispensables para la gestión de documentos e información en sistemas informáticos y para los documentos de archivo que se gestionan en soporte papel en las unidades de archivo de las organizaciones. Sin una correcta gestión de los documentos e información, se corre el riesgo de incurrir en violentar los derechos de las personas, perder información vital para la organización o para hacer valer derechos ciudadanos, e incluso como se ha visto

recientemente, las funciones institucionales y los servicios que se brindan a la población se pueden ver afectadas tras la carencia de un desarrollo más integral de los sistemas de gestión de documentos electrónicos.

7. CONCLUSIONES

A modo de conclusión, se considera necesario que la ciberseguridad en Costa Rica mejore sus prácticas en materia de seguridad de la información, ya que de esto depende que los datos de los distintos usuarios de las plataformas y sistemas a nivel país se encuentren seguros. Para ello se debe acatar la normativa en relación con la seguridad y protección de datos personales con el fin de proteger el derecho de intimidad de las personas en cuanto al manejo de su información personal.

Además; es importante destacar la relevancia y prioridad con la que debe abordarse el tema de la ciberseguridad en Costa Rica; especialmente por la reciente ola de ataques que comprometen la seguridad de la información en varias instituciones públicas. El accionar gubernamental debe avocarse a proteger y custodiar de la mejor manera los activos de la información, y para esto resulta imprescindible la creación de grupos de trabajo intersectoriales e interdisciplinarios que tracen la ruta a seguir de forma que se evidencie una pronta mejoría.

Finalmente, y a través de todo lo analizado en el presente artículo, se espera incentivar en las personas lectoras de este texto, y sobre todo en el gremio de profesionales en Archivística, que se involucren en materia de ciberseguridad, ya que esto es una parte fundamental para la protección de los derechos de las personas a través de la gestión de los documentos, y garantizar que estos se encuentren seguros y accesibles para las partes interesadas según los fines para los cuales fueron creados. La pérdida de información podría suponer la pérdida de fuentes y recursos que permitan cumplimentar los derechos de la ciudadanía.

8. REFERENCIAS BIBLIOGRÁFICAS

Carta de los Derechos Fundamentales de la Unión Europea. (2000): https://www.seaus.net/images/stories/pdf/Carta_de_Derechos_Fundamentales-UE.pdf

CISCO. (2021). ¿Qué es la ciberseguridad?: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Comité Interministerial sobre Ciberseguridad. (2017). Política nacional de ciberseguridad. Santiago, Chile: https://biblioteca.digital.gob.cl/handle/123456789/738

Constitución Política de la República de Costa Rica. (1949). Costa Rica: https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=871

Fonseca, J. M. C., & Juárez, B. Z. (2019). Ciberseguridad y vigilancia tecnológica: un reto para la protección de datos personales en los archivos. Tlatemoani: revista académica de investigación, 10(31), 218-246: https://dialnet.unirioja.es/servlet/articulo?codigo=7295555

Galán, C. & Galán C., C. (2016). La ciberseguridad pública como garantía del ejercicio de derechos. Derecho & Sociedad, 47, 293-306: https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/18892

Leiva, E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. Revista Latinoamericana de Ingeniería de Software, 3(4), 161-176: http://revistas.unla.edu.ar/software/article/view/775

Ley No. 8968 de 2011. Protección de la Persona frente al tratamiento de sus datos personales. 5 de septiembre de 2011: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989

Maroto, J. P. (2009). El ciber espionaje y la ciberseguridad. In La violencia del siglo XXI. Nuevas dimensiones de la guerra (pp. 45-76). Instituto Español de Estudios Estratégicos.

Moreno, A. H. (2017). Ciberseguridad y confianza en el ámbito digital. Información Comercial Española, ICE: revista de economía, (897), 55-6 https://dialnet.unirioja.es/servlet/articulo?codigo=6265462

Reyes Prado, A. (s.f.). ¿Por qué tenemos derechos humanos?: https://www.corteidh.or.cr/tablas/R22848.pdf

Serrano, S., Vázquez, D. (2011). Fundamentos teóricos de los derechos humanos.https://piensadh.cdhdf.org.mx/images/publicaciones/material_de_capacitacion/curso/2011_Fundamentos_teoricos_dh.pdf

Unión Interparlamentaria. (2016). Derechos Humanos: https://www.ohchr.org/sites/default/files/Documents/Publications/HandbookParliamentarians_SP.pdf

Voutsáas M., J. (2010). "Preservación Documental Digital y Seguridad Informática." Investigación Bibliotecológica. Centro Universitario de Investigaciones Bibliotecológicas, UNAM. (Vol. 24, no. 49.) http://www.interpares.org/display_file.cfm?doc=ip3_mexico_dissemination_b_c_voutsass_archivos-electr%C3%B3nicos_2011.pdf



SOBRE LA REVISTA DEL ARCHIVO NACIONAL DE COSTA RICA

La Revista del Archivo Nacional (RAN) se dirige a profesionales de Archivística y Ciencias afines, y a personas vinculadas con el quehacer de los archivos y con sus temáticas centrales. Se encuentra incluida en Latindex, Sistema Regional de Información en Línea para Revistas Científicas de América Latina, el Caribe, España y Portugal. Se produce un volumen cada año.

Sección ARCHIVÍSTICA

Se publican artículos especializados en esta ciencia, que es el corazón mismo de la RAN. No importa si el tema se conecta con otras especialidades; si su tema principal es algún aspecto del quehacer archivístico, es posible publicarlo en esta sección.

Sección CIENCIAS AFINES

La RAN abre también sus páginas a profesionales de otras carreras, siempre que se trate de textos que de alguna forma se vinculen con el quehacer de los archivos.

Sección PRISMA

Esta es una sección más flexible en la que se publican aportes como experiencias de difusión del patrimonio, estudios de casos, sistematizaciones y opiniones técnicas de proyectos destacados, entre otros.

Sección DOSSIER MONOGRÁFICO

Sección administrada por la Comisión Editora. Cada año se selecciona un tema específico y se invita a personas expertas a desarrollar textos especializados en la materia respectiva.

¿Desea publicar su trabajo?

INGRESE AQUÍ

Revista del Archivo Nacional de Costa Rica
ISSN 2215-5600
www.archivonacional.go.cr/RAN

Ministerio de Cultura y Juventud
Archivo Nacional
Vivir Cultura es Crecer como país
2022-2026 Costa Rica Trabajando, decidiendo, mejorando