UNIVERSIDAD CENTRAL DE VENEZUELA

FACULTAD DE HUMANIDADES Y EDUCACIÓN

ESCUELA DE BIBLIOTECOLOGÍA Y ARCHIVOLOGÍA

PROPUESTA DE LINEAMIENTOS PARA LA PROTECCIÓN DE LA INFORMACIÓN DIGITAL.

Trabajo de licenciatura presentado ante la Universidad Central de Venezuela para optar al título de licenciado en Bibliotecología.

Juan Carlos Silva Gil.

TUTOR: Prof. José López

Caracas, julio de 2015

Silva Gil, Juan Carlos

Propuesta de lineamientos para la protección de la información digital / Juan Carlos Silva Gil; Tutor López. Jose .– Caracas, 2015

ix, 125 p.; figs., tabs., .

Tesis (Licenciatura en Bibliotecología) – Universidad Central de Venezuela, Facultad de Humanidades y Educación, Escuela de Bibliotecología y Archivología.

1. Bibliotecología. 2. Lineamientos. 3. Protección 4. Información digital.. I.Título. II. López, Jose, Tutor

AGRADECIMIENTOS

Cerrando este ciclo quiero dedicar unas palabras a todos los que me han hecho posible, y digo eso no por mala redacción, ya que cada interacción, cada palabra, cada experiencia que compartí con cualquier conocido me ha hecho lo que soy, para bien o para mal.

Quiero agradecer a mis seres queridos que ya no están con nosotros, a mi abuelo Hugo, a mi abuelo Felipe y a mi abuela Josefina por dar los valores y el amor a quienes me los han dado a mí, a mi tía Sofía que más que ser la primera Miss Venezuela fue una dulzura siempre con historias divertidas, a mi tía María Jesús, porque siento que herede de ella mis dotes poéticos y a mi tío Antonio con quien compartí mucho en las buenas y en las malas y me enseño a mejorar mi discurso intelectual.

A mi "trio de la seguridad", Carolina Uban, Franyoli Gomis y Balby Mora porque siempre me alegran con verlas, a Jenny Beatriz Landaeta Rodríguez por escucharme y permitirme aprender de tu constancia, a mis hermanos fuera de lo consanguíneo Marcos Prato y Marco Antonio Vilera porque siempre me han brindado su apoyo en momentos oscuros y a mi segunda madre Betty Prato.

De la Universidad a todos mis compañeros mientras hacía vida en la universidad, en especial a Wilhen Vielma y a Reynaldo José por tenderme la mano en momentos inesperados, agradezco también a todos los profesores de la EBA por ser parte de mi formación, a la profesora Mariketi Papatzikos porque me protegió como una madre y sobre todo a mi tutor y amigo el profesor José López quien desde la primera clase de Catalogación me ha enseñado a indagar y a perder el miedo de enfrentarlo como profesor si investigaba lo suficiente para validar mi argumento.

A mi abuela Herminia por su cariño y porque siempre seré su "negrito"

A mi hermano Hugo porque sé que no es fácil lidiar conmigo, a mis tíos porque son otros padres que siempre me han dado afecto, cuidado y consejo, también a todos mis primos pues nos criamos como hermanos.

Y por último a mi padre y a mi madre, y los coloco de últimos no por ser menos importantes sino porque ustedes son la epítome de mi historia, el amor, la dedicación, los valores y la fuerza que me han dado por años se puede resumir en una frase. Gracias por siempre creer en mi más que yo mismo.

Alma Mater floreat quae nos educavit (que florezca la universidad que nos ha educado)

CONTENIDO

PÁG

RESUMEN viii

INTRODUCCIÓN 1

CAPÍTULO I – El problema 5

1.1.- Planteamiento del problema 5

1.2.- Objetivo general 8

1.3.- Objetivos específicos 8

1.4.- Justificación e importancia de la investigación 8

1.5.- Ubicación en el contexto acumulado 10

CAPÍTULO II – Marco teórico referencial 11

2.1.- Antecedente de la investigación. 11

2.2.- Bases teóricas: 12

2.2.1.- Conceptos de información 12

2.2.1.1.- Información electrónica 12

2.2.1.2.- Información digital 13

2.2.1.3.- Propiedades de la información digital 13

2.2.2.-Protección, conservación o preservación de información 15

2.2.2.1.- Protección-preservación-conservación 15

2.3.-Preservacion de lo analógico a largo plazo. 17

2.3.1.-De lo análogo a lo digital 19

2.4.- Preservación digital 22

2.4.1.- Metadatos para la preservación digital. 26

CAPÍTULO III – Marco metodológico 28

3.1.- Tipo de investigación: 28

3.2.- Diseño de investigación: 28

3.3.- Población-muestra: 28

3.4.- Técnica e instrumentos de recolección de datos: 29

3.5.- Técnica de análisis y representación de los datos: 29

CAPÍTULO IV – Análisis contextual 30

4.1- Paradigmas 30

4.1.1.- El paradigma físico: 31

4.1.2.- El paradigma cognitivo: 34

4.1.3- El paradigma social: 37

4.1.4- Paradigma actual de la Bibliotecología. 39

4.2.- Los factores de preservación de la información digital. 45

4.2.1.- Estructura jurídico-legal de la información. 45

4.2.2.- Derecho de autor: 45

4.2.3.- Patentes de invención: 48

4.2.4.- Protección legal: 49

4.2.5.- Nuevos formatos emergentes 51

4.2.6.- Preservación digital: 52

4.3.- Aspectos tecnológicos de la protección de la información digital 54

4.3.1.- Problemas de hardware 54

4.3.2.- Errores de software: 56

4.3.3.- Errores humanos: 63

4.3.4.- Software malicioso 64

4.3.5.- Incidencias del entorno: 65

4.4.- Los métodos más eficientes de protección de la información digital 66

4.4.1.- La nube (cloud computing): 66

4.4.2.- Discos duros: 69

4.4.3.- Encriptado: 71

4.4.4.- Respaldos de información: 79

CAPÍTULO V - LINEAMIENTOS PARA LA PROTECCIÓN DE LA INFORMACIÓN DIGITAL 85

Lineamientos de protección de la información digital 85
5.1.- Protección legal: 86
5.2.- Preservación digital: 87
5.2.1- La nube: 87
5.3.- Aspectos tecnológicos de la protección de la información digital 89
5.3.1.- Problemas de Hardware 89
5.3.2.- Errores de software: 91
5.4.- Errores humanos: 92
5.5.- Incidencias del entorno: 95
5.6.- Consideraciones adicionales. 96
5.6.1.- Discos Duros: 96
5.6.2.- Encriptado: 97
5.6.3.- Respaldos de información: 97
5.6.4.- Movilidad de la información digital: 98
5.6.5.- Antivirus: 99
5.6.6.- Estudio de Metadatos de preservación: 100
5.6.7.- Emulación: 101
CONCLUSIONES 102
RECOMENDACIONES 104
BIBLIOGRAFÌA 106

INDICE DE TABLAS Y FIGURAS

Tabla 1.Lista de errores y debilidades de software 59

Tabla 2.Lista de errores por interacción insegura de componente 60

Tabla 3.5 Lista de errores por gestión de recursos riesgosos 61

Tabla 4.Lista de errores consideradas defensas porosas 61

Tabla 5.Tabla comparativa de ventajas y desventajas del disco duro magnético 69

Tabla 6.Tabla comparativa de ventajas y desventajas del disco rígido 70

Tabla 7.Ejemplo de tabla de codificación del cifrador de polybios 72

Tabla 8.Tabla codificadora del sistema de cifrado de César 73

Tabla 9.Tabla explicativa de uso del criptosistema de Vigenére 75

Tabla 10.Tabla ejemplo del criptosistema de Vigenére 76

Tabla 11.Tabla de asignación de valores a la representación en grados para su equivalencia en bit 77

Tabla 12.Tabla explicativa de valores aceptados por cada tipo de ristra de bits 78

Tabla 13.Tabla explicativa del funcionamiento del proceso de encriptado cuántico 78

Figura 1. Explicación grafica de la información conveniente 41

Figura 2. Principales factores que causan una perdida de información, tomado de 53

Figura 3. Representación gráfica de una escitala con mensaje encriptado 71

Figura 4.Representación gráfica disco de Alberti 74

Figura 5.Esquema de los lineamientos propuestos como resultado de la investigación 86

RESUMEN

PROPUESTA DE LINEAMIENTOS PARA LA PROTECCIÓN DE LA INFORMACIÓN DIGITAL.

Autor: Juan Carlos Silva Gil.

Tutor: Prof. José López

Luego de la revolución industrial, la incursión de tecnologías analógicas-electrónicas y la llegada de la era digital estamos frente a un evento que si bien supone una oportunidad enorme de crecimiento para la bibliotecología, un descuido o atraso en la adaptación de procedimientos de protección almacenamiento, acceso y reproducción de información digital podría estancar los avances en áreas importantes como sistemas de catalogación digital, sistemas de recuperación de información, certificados digitales e incluso en la capacitación de los profesionales de la información.

El entorno digital es para muchos un milagro tecnológico. Una piedra filosofal en la difusión de la información que supero a la imprenta de Gutenberg y con requerimientos de espacio muy pequeños para su almacenamiento, sin embargo su fragilidad radica en la facilidad con la que se puede comprometer su integridad, de contenido o confidencialidad. Es por ello que se ha convertido en el objeto de estudio de esta investigación.

El desarrollo de este proyecto se definió como no experimental transeccional descriptiva y documental. Por definición, es un modelo de investigación en el que no se manipulan variables intencionalmente, consiste en proporcionar una visión de un contexto o situación para después analizarlos, claro está, basándose en la documentación estudiada y citada con el fin de elaborar de una propuesta viable para solventar los problemas planteados.

La presente investigación propone diseñar lineamientos que permitan proteger la información en materia de acceso y de conservación para cualquier formato digital. Al denotar las necesidades del paradigma actual de la bibliotecología en el área digital, sus factores de preservación y los métodos más eficientes para su protección, se logró tener una visión general de la situación y diseñar lineamientos que consolidaron el objetivo planteado.

INTRODUCCIÓN

La importancia de la información desde tiempos antiguos es innegable, no solamente nos mantiene al tanto de la historia y nos ayuda con los avances tecnológicos sino que gerencialmente nos ayuda en el proceso de toma de decisiones. Esto va desde una simple comparación de una información con un hecho concreto, hasta un análisis DOFA para lograr mejoras en cualquier Institución.

En nuestra realidad actual el auge de la información a nivel mundial sobrepasa por mucho las estadísticas anteriores, se ha calculado la información global desde 1986 hasta el año 2007 y el crecimiento es bastante notable, se pasó de 2,6 exabytes en 1986 a 295 exabytes en el 2007.

Estaríamos hablando de miles y miles de millones de Gigabytes, que es una medida más manejada por el usuario común y aun cuando cerca de un 25 a 30% de toda la información en internet está duplicada, observamos que la cantidad de información que debemos proteger como profesionales en esta área puede salir de nuestras manos fácilmente si no nos adaptamos a nuevas medidas y procedimientos.

La protección de la información hasta ahora se ha enfocado mayormente en conservar los soportes de información a través del tiempo, pero eso ya no es suficiente. Los soportes actuales claramente ofrecen algunas ventajas inigualables a los soportes analógicos clásicos, sin embargo también presentan unas desventajas muy fuertes para el paradigma actual. Entre ellas la obsolescencia digital, el cambio continuo en la estructura del hardware y software (lo que lo haría menos intuitivo), limitaciones al acceso de nuevas tecnologías y la diferencia entre distintos sistemas con objetivos similares, que dividen el mercado y a su vez aumentan el tiempo de aprendizaje necesario. Las desventajas irán aumentando a medida que avance la tecnología por lo que podríamos esperar que esas desventajas también crecerán a niveles exponenciales.

Es por el desbalance en crecimiento, que se establece como objetivo, crear lineamientos para la protección de la información digital en búsqueda de una normalización de procedimientos que ataquen las desventajas del entorno digital. Para ello debimos: analizar el paradigma

actual de la bibliotecología y abordar las carencias en torno a las necesidades actuales, los factores más influyentes en la preservación de la información digital para conocer si existen elementos que se hayan dejado de lado en los procedimientos ya normados e identificar los métodos más eficientes de protección de la información digital, para lograr de manera acertada contrarrestar las fallas de los métodos de protección tradicionales aplicados al entorno digital.

Con estos lineamientos se espera disminuir la pérdida de la información digital y concientizar a los profesionales de la información en considerar la protección de la información un tema enfocado en lo intangible, sin olvidar claro la importancia de los métodos actuales y su influencia en la actualidad.

Desde hace años se han presentado distintos programas y proyectos dedicados a abordar los problemas de preservación que presentan un enfoque meramente físico de la información, sin embargo algunos proyectos si han buscado establecer un estándar técnico para los métodos en la preservación por medio de la digitalización. Se han analizado las ideas de patrimonio y preservación digital para lograr comprender los programas con dicho fin y cómo gestionarlos, observando elementos como toma de decisiones sobre qué debemos conservar, la colaboración con los productores de información, los metadatos, la protección y la accesibilidad de la información.

Incluso se han planteado estrategias para mejorar el acceso a la información digital. Con puntos claves como la reusabilidad de la información, buscar una forma de representar el formato original para conservar la sensación analógica de la información y migrarla a formatos actuales para evitar la obsolescencia y tener una alta adaptación a la preferencia de los usuarios.

En este trabajo podremos encontrar la justificación del planteamiento del porqué existe la necesidad de crear unos lineamientos de protección de la información digital, apoyadas en un marco teórico donde observaremos más a fondo algunos de los antecedentes ya mencionados, las bases teóricas para comprender la diferencia entre la protección, preservación y conservación de la información, y la preservación aplicado al mundo digital. Y luego de indicar el tipo de investigación en el capítulo IV se empieza a relacionar esas necesidades y

conceptos con los objetivos planteados para mostrar en el capítulo V el resultado de este trabajo: Los lineamientos para la protección digital seguido de unas recomendaciones.

La protección de la información es un tema muy amplio en aspectos como: los paradigmas, la protección jurídico-legal, la preservación digital, sistemas de almacenamiento y técnicas para respaldo y recuperación de la información, por ello el alcance de este trabajo de investigación y los lineamientos resultantes están enfocados en el área de la bibliotecología.

La construcción de esta investigación se basó en una primera instancia en los parámetros metodológicos propuestos del Manual para la Elaboración, Presentación y Evaluación del Trabajo de Licenciatura de la Escuela de Bibliotecología y Archivología de la Universidad Central de Venezuela. Para una mejor comprensión por parte del lector, la investigación se dividió en cinco partes, establecidos de la siguiente manera:

CAPÍTULO I – El problema: En este capítulo se exponen las deficiencias que posee el paradigma actual de la bibliotecología, las desventajas de los medios digitales y referencias a trabajos de investigación de otros autores que aportan avances en materia de protección de la información digital. Planteando así la justificación para esta investigación.

CAPÍTULO II – Marco teórico referencial: En este capítulo se establecen las bases teóricas de la investigación. se expuso los conceptos, definiciones y teorías relativas a la protección de la información, las diferencias entre términos como protección, preservación y conservación, así como las propiedades de la información digital y un paseo muy breve por los sistemas precursores de la digitalización.

CAPÍTULO III – Marco metodológico: En este capítulo se presenta la metodología que fue utilizada para llevar a cabo esta investigación, Se determina su tipo y diseño, atendiendo a las necesidades planteadas en el problema. Además se presentan la población y muestra escogidas y el instrumento para la recolección, análisis y representación de los datos, permitiendo así al lector obtener una mejor comprensión de los procesos de la investigación.

CAPÍTULO IV – Análisis contextual: Este capítulo tiene como fin exponer la situación del paradigma actual de la bibliotecología, analizar los factores de preservación de la información

digital e identificar los métodos más eficientes de protección de la información digital. Para seguir los procedimientos de los objetivos específicos mencionados anteriormente.

CAPÍTULO V - LINEAMIENTOS PARA LA PROTECCIÓN DE LA INFORMACIÓN DIGITAL: Este último capítulo se presenta el producto final de la investigación, basado en los análisis de los estudios ya realizados, y diferentes maneras de abordar la protección digital consideradas por distintos autores en otras partes del mundo; así como en los análisis realizados en los capítulos anteriores sobre las carencias en los procedimientos normados para evitar la pérdida de la información digital.

CAPÍTULO I – El problema

1.1.- Planteamiento del problema

En la actualidad la bibliotecología en materia de conservación enfoca sus métodos mayormente en el resguardo de los soportes, si bien es cierto que bajo este enfoque la preservación del material es necesaria para el entorno análogo, no podemos negar la influencia de la tecnología en nuestra área. No negamos que el papel es uno de los soportes más resistentes al tiempo, que requiere de menos recursos para ser usado dado a que su decodificación no depende más que de la lectura y el lenguaje de quien busca información, ventaja inigualable a cualquier soporte electrónico con una desventaja que el mundo globalizado no perdona, la accesibilidad y reproducción limitada.

La preservación en los medios tradicionales tiene varias desventajas notables, el proceso de chequeo y mantenimiento del material es considerablemente extenso dependiendo del tamaño de la colección y la cantidad de personal dedicada a la tarea, cualquier plan de remodelación para la unidad de información requiere la movilización del material y planes de resguardo en el periodo de la remodelación negando el acceso a los usuarios, el deterioro aun cuando lento es inevitable por su uso, al poseer todas las copias de los ejemplares en una misma localización corre el riesgo de la pérdida de todos los ejemplares ante un desastre (incendio, inundación, terremoto), la ubicación de los ejemplares en la estantería tiene un margen de error que se traduce en tiempo perdido al recuperar información si el ejemplar no es devuelto a su lugar exacto, en caso de una pérdida o daño grave al material su reposición es costosa.

Las bibliotecas venezolanas actualmente poseen manuales de preservación de soportes (CONSERVAPLAN) que incluyen en el manejo de emergencias aspectos como: daño por agua e incendio, agentes biológicos, hurto, control integral de plagas, protección contra hongos entre otros temas de preservación que concierne a las bibliotecas y son de importancia absoluta. Pero sobre la preservación digital de información muchas de las instituciones venezolanas tienen una falsa concepción o quizás incompleta, se cree que basta con la migración de un soporte analógico a uno digital por medio de la digitalización para lograr el objetivo, y aun cuando la digitalización es una parte muy importante, es solo un paso o aplican los mismos criterios tradicionales para los soportes de almacenamiento digital (CD-

ROM, DVD, entre otros). Dicha consideración sobre la preservación deja de lado los aspectos sobre la intangibilidad señalada por Hilde van Wijngaarden (2008) y Codina (2001).

Desde hace años que se presentaron los objetos digitales *"Materiales digitales* se utiliza aquí como término preferido para englobar los diferentes elementos constitutivos del patrimonio digital en general. En algunos casos, también se utiliza *objeto digital* o *recurso digital*. Estos términos se emplean de manera intercambiable y genérica" (Biblioteca Nacional de Australia, 2003, p.21)

Existen cinco aspectos básicos de un objeto digital refiriéndose a aspectos como su codificación (contenido), el código de comportamiento ante un estado especifico del objeto (comportamiento), el diseño visual del objeto (apariencia), qué función ejerce el objeto, autoría, relación con otros objetos digitales (contexto) y a cómo se muestra el contenido de (estructura). (Wijngaarden, 2008, p.6)

Es difícil decir con certeza dentro del paradigma bibliotecológico que es la preservación digital sin adentrarnos en los tecnicismos que esto conlleva, de manera breve la UNESCO en un documento preparado por la Biblioteca Nacional de Australia define la preservación digital de la siguiente manera:

> La preservación digital consiste en los procesos destinados a garantizar la accesibilidad permanente de los objetos digitales. Para ello, es necesario encontrar las maneras de representar lo que se había presentado originalmente a los usuarios mediante un conjunto de equipos y programas informáticos que permiten procesar los datos. Para lograrlo, es necesario que la comprensión y la gestión de los objetos digitales se realice considerándolos desde cuatro puntos de vista: como fenómenos físicos, como codificaciones lógicas, como objetos conceptuales comprensibles para el ser humano y como conjuntos de elementos esenciales que deben ser preservados para ofrecer a los futuros usuarios lo esencial del objeto. (Biblioteca Nacional de Australia, 2003, p.37)

Algunos documentos digitales como revistas, fotografías, videos entre otros que también se encontraban en soporte analógico se han adaptado para pasar a otra modalidad de trabajo bajo

un ambiente meramente digital que les resulta más económico, rápido y eficiente, a las unidades productoras y administradoras de información, como es el caso de la Enciclopedia Británica que dejo atrás su versión impresa y ahora trabaja solo de manera digital.

Para evitar confusión en los términos debemos aclarar la diferencia entre tres aspectos distintos de la información, lo virtual, lo digital y lo electrónico

Lo virtual:

La virtualidad de la información según Codina no es más que "algo que existe en una forma diferente a lo habitual compuesto por bits y no por átomos, pero existe" (Codina, 2001, p.3). Podemos decir que es un ambiente electrónico no material (en sentido físico) originado por y para tecnologías digitales hospedado en la web, accesible desde cualquier dispositivo con internet que nos da la posibilidad de interactuar con ese entorno virtual.

Lo digital:

La información digital tiene ciertas cualidades: es computable, refiriéndose esto a la posibilidad de ser procesado por una computadora mediante algoritmos binarios (ceros y unos) "Para que la información pueda considerarse totalmente digital ha de ser emitida, distribuida y recibida digitalmente, lo cual sólo se puede hacer mediante los sistemas online, que en realidad tampoco son tales necesariamente." (Sanjuán, 2001, p.16)

Lo electrónico:

"Documento electrónico: aquel documento que precisa de una máquina que funcione de forma electrónica, sea análoga o digital, para poder ser producido o visualizado." (Rodríguez, 2010, p.17) con esta definición podemos entender que existen elementos electrónico-analógico (un casete) y electrónico-digital (un documento de Excel)

En esta investigación se establecen los elementos o factores a tomar en cuenta en la formulación de lineamientos para la preservación de la información digital.

1.2.- Objetivo general

Proponer lineamientos para la protección de la información digital.

1.3.- Objetivos específicos

Caracterizar el paradigma actual de la bibliotecología y su desempeño en la protección de la información.

Analizar los factores de preservación de la información digital.

Identificar los métodos más eficientes de protección de la información digital.

1.4.- Justificación e importancia de la investigación

Los lineamientos son directrices, acciones específicas a seguir que determinan el cómo, por qué y para qué ejecutar esas acciones referentes a un tema que comúnmente se repite en diferentes circunstancias, buscando crear procesos estandarizados para solucionar un problema. En el caso de la preservación de información, es necesario que existan lineamientos para todas las instancias donde encontremos información, que puede ser análoga o digital, en lo que concierne a lineamientos para información analógica ya encontramos documentos altamente conocidos emitidos por las autoridades internacionales del área de la información como la IFLA, aceptadas y aplicadas como un estándar en bibliotecas de todo el mundo. Con el auge de la información digital es preciso diseñar lineamientos para la preservación de la información digital, hacer lo necesario para su difusión y adaptación para lograr su estandarización.

La investigación presenta el paradigma actual de la bibliotecología respecto a la protección enfocada solo en los soportes, el uso de herramientas tecnológicas para tales fines y los planes de conservación actuales usados como norma en todo el país; se analizará el paradigma actual respecto a los aspectos de preservación de la información y se expondrá las virtudes de la

información digital y sus ventajas en la protección de la información. Esto por tres razones fundamentales: 1.) El gran alcance de las nuevas tecnologías tanto en la creación como en la administración de información. 2.) La fragilidad digital y 3.) La rápida obsolescencia de los sistemas (software y hardware).

En plan de darle una vida útil más extendida a la información se diseñaran lineamientos de protección de información digital

En algunas instituciones Venezolanas creen realizar avances en materia de preservación digital de información, cuando solo tienen planes de digitalización con lo que asumen lograr el objetivo, y aun cuando la digitalización es una parte muy importante, es solo un paso.

Existen cinco aspectos básicos de un objeto digital: estructura, contexto, apariencia, comportamiento y contenido (Wijngaarden, 2008). Dado que la información que nos da un objeto no se limita a lo que este escrito o descrito en él, debemos pensar en preservar toda la información que el documento proporcione incluyendo toda reacción a su percepción. Para dar una explicación más clara, aun cuando una fotografía digital pueda captar cada detalle de un lugar y demos una descripción detallada del entorno no se experimenta de la misma forma que ir al lugar, verlo con nuestros propios ojos, sentir el clima frío o cálido, húmedo o seco, al igual que sucede con una obra de un museo, escultura, pintura o fotografía.

La importancia de preservar la información digital no está solo en su acceso, si la información digital mantiene los cinco aspectos mencionados anteriormente da una mayor fidelidad a toda la información que puede ser obtenida de ese objeto digital, al igual que con los documentos físicos en algunas ocasiones el enfoque de los planes de preservación digital irán enfocadas a un área en particular "Al escoger un método de preservación digital en particular, determinamos que aspectos de esa entidad son preservados y cuáles serán sacrificados." (Traducción propia)[1]

[1] we determine which aspects of such entities will be preserved and which ones will be sacrificed. (Rothenberg, 1995, p.55).

1.5.- Ubicación en el contexto acumulado

La investigación presenta se enmarca dentro de las líneas 4 y 5 desarrolladas por CIDECI: 4 que aborda el estudio del impacto de las nuevas tecnologías en el campo de la comunicación de la información y 5 el procesamiento, almacenamiento y recuperación de la información.

CAPÍTULO II – Marco teórico referencial

2.1.- Antecedente de la investigación.

Se observó que en las bases de datos de SABER UCV y SISTEMA DE PUBLICACIÓN ELECTRÓNICA DE TESIS Y DISERTACIONES de La Universidad del Zulia (LUZ) no se encontraron trabajos de grado en los que se estudiase el tema de la protección de la información digital, por ello no se contó con antecedentes previos para esta investigación.

Consideraciones generales

-En el año 2003 la UNESCO presentó un documento preparado por la biblioteca nacional de Australia titulado *Directrices Para La Preservación Del Patrimonio Digital.* Allí se analizan las ideas de patrimonio y preservación digital para lograr comprender los programas con dicho fin y como gestionarlos, observando elementos como toma de decisiones sobre qué debemos conservar, la colaboración con los productores de información, los metadatos, la protección y la accesibilidad de la información.

-En marzo del año 2006 la *National Diet Library (NDL)* de Japón presentaron el sexto reporte de investigación sobre la preservación digital en un documento titulado *The long-term Accessibility of Packaged Digital Publications* (La accesibilidad a largo plazo de unidades de publicaciones digitales). En ese informe reconocen los avances tecnológicos en áreas de la información digital por lo que se plantean que quizás en términos de una generación con el avance tan acelerado de la tecnología los métodos de acceso a esa información se vuelvan obsoletos y perdamos la capacidad de reproducirlos lo que los impulso a realizar este estudio

- El programa nacional para la preservación del papel en los Países Bajos: *Metamorfoze* (1997) creó un proyecto denominado “preservation imaging” y presentó ante la IFLA en el año 2007 un borrador basado en la conversión digital de materiales en microfilm titulado *Guidelines Preservation Imaging Metamorfoze.* Con este proyecto se buscaba establecer un estándar técnico para los métodos en la preservación (de microfilms) por medio de la digitalización.

-Hilde van Wijngaarden quien fue jefe del departamento de preservación digital de la Biblioteca Nacional de los Países Bajos en el 2008 en su presentación *Preservation Action: What, how and when?* plantea estrategias para retomar o mejorar el acceso a información digital estableciendo como metas: la mejora en la accesibilidad de la información, la reusabilidad de la información para conservar su funcionalidad, buscar la forma de representar el formato original para conservar la sensación del soporte analógico, migración a formatos actuales para evitar la obsolescencia de software y adaptarse a las preferencias de los usuarios.

2.2.- Bases teóricas:

2.2.1.- Conceptos de información

Información: "La información es un conjunto de mecanismos que permiten al individuo retomar los datos de su ambiente y estructurarlos de una manera determina, de modo que le sirvan como guía de su acción" (Paoli, 1989, p.15 c.p Jiménez, 2005)

Documento: "Toda información fijada sobre un soporte y susceptible a ser recuperada" (Calderón, 2006, p.1)

Viendo esto podemos decir que la principal diferencia entre los dos conceptos es que la información contiene datos y no necesita un soporte, y el documento contiene información fijada en algún soporte físico sin importar su tipo

2.2.1.1.- Información electrónica

En el documento titulado La validación de los documentos: pasado, presente y futuro plantea: "se denomina documento electrónico a cualquier entidad de información que es accesible a través de un medio electrónico, y digo accesible, no generado". (Díaz, 2007, p.135)

Esto podría causar una duda razonable, muchos confunden un medio electrónico con uno digital, pero para esclarecer un poco esa duda en el documento titulado Las nuevas entidades de información analizadas desde la perspectiva de la organización de la información define:

“Documento electrónico: aquel documento que precisa de una máquina que funcione de forma electrónica, sea análoga o digital, para poder ser producido o visualizado.” (Rodríguez, 2010, p.17) con esto podemos ya ver una diferencia clara con la existencia de documentos electrónicos-analógicos y electrónicos-digitales, “Aunque los términos se están acuñando popularmente con muchas rapidez, en estricto sentido la información digital está comprendida dentro de la información electrónica, no son por tanto sinónimos.” (Sanjuán, 2001, p.16) después de presentadas estas ideas sería acertado decir que toda información digital es electrónica, pero no toda información electrónica es digital.

2.2.1.2.- Información digital

Para hablar del concepto de información digital, comenzaremos por leer un fragmento del artículo Las propiedades de la información digital:

Decimos que una información es digital cuando está codificada en el formato que puede interpretar un ordenador y suele decirse que consiste en series de ceros y de unos. Pero esto, aunque útil, no deja de ser una simplificación. (Codina, 2001, p.1).

Siguiendo la misma idea “El concepto de información digital se aplica para todo aquello representado mediante ceros y unos dentro de una computadora” (Carrión, 2007). Con este concepto debemos entender que: “La información digital no sólo son textos electrónicos, también se incluyen las imágenes, el audio y el video, que al igual que los textos tienen diferentes formatos, codificaciones y representaciones en el mundo electrónico”. (Carrión, 2007, p.4). Sabiendo que “Para que la información pueda considerarse totalmente digital ha de ser emitida, distribuida y recibida digitalmente, lo cual sólo se puede hacer mediante los sistemas online, que en realidad tampoco son tales necesariamente.” (Sanjuán, 2001, p.16)

2.2.1.3.- Propiedades de la información digital

Existen tres características básicas de la información digital: la computabilidad, la virtualidad y la capacidad (Codina, 2001, p.2). La computabilidad es la propiedad de todo archivo digital que requiere de un hardware y un software para ser procesable (legible) a nivel humano y como otros métodos de registro de información su principal objetivo es el de

recuperar la información con una gran ventaja, con ayuda de algoritmos podemos realizar búsquedas que serían casi imposibles con material analógico, buscar una frase completa, excluir palabras de un texto, buscar archivos por campos registrados en una base de datos entre otros.

La virtualidad, es un concepto que ha cambiado mucho, ya virtual no necesariamente es algo de existencia ficticia o de existencia aparente, el concepto de lo virtual integrado a la era digital nos indica que eso existe sin las limitaciones de lo analógico. Codina nos recuerda algunas consecuencias directas y muy diferentes de información en bits (digital) y la información en soporte físico "registrada mediante átomos" (Negroponte, 1995).

La virtualidad en la información le da una gran ventaja, económicamente el costo por una copia digital de la misma información es cero (en términos de procesos) pero a su vez nos trae un problema que es el ruido; La gran cantidad de información repetitiva que encontramos en internet junto con información que no tiene una fuente fiable (que también se vuelve repetitiva) por lo que cada vez es más necesaria la presencia de un profesional de la información en una institución que produzca o distribuya información.

Otro problema que nos menciona Codina se refiere a la dificultad de determinar los límites de un documento por sus cualidades multimedia, documentos con textos que a su vez pueden contener videos, imágenes en grandes cantidades, elementos interactivos o archivos de sonido por lo que considera que podemos encontrar problemas para identificar, acceder y preservar documentos digitales de manera adecuada.

La capacidad es un aspecto que los profesionales de la información siempre deben tomar en cuenta y afecta casi a todas las decisiones en cuanto a la dirección de una biblioteca, ¿Qué libros pueden ser retirados para dar espacio a las nuevas ediciones? ¿Cuántos ejemplares debo mantener de cada título? ¿Debo guiarme solo por las estadísticas de uso para retirar títulos? ¿Cuánto espacio necesito para mi archivo histórico?, esas y más preguntas no suelen ser necesarias para información digital, dado a que la cantidad de contenido que pueda poseer un documento no afecta significativamente el espacio físico que ocupa, un ejemplo muy claro que nos presenta Codina es la "Internet movie data base" (Codina, 2001, p.5) la cual es una base de datos cinematográfica en internet, que incluye biografías de actores, actrices,

directores y más de 200 mil películas; Información que sería prácticamente imposible de recopilar en un solo ejemplar.

2.2.2.-Protección, conservación o preservación de información

Aun cuando protección, conservación y preservación son conceptos diferentes pero relacionados entre sí, tienen un punto fundamental en común: cuidar, proteger, evitar daño o peligro, incluso aquellos que vienen con el paso del tiempo, en el caso de la información como ente intangible, ¿Qué peligro corre? ¿Cómo se daña o pierde? Principalmente, perdiendo su soporte.

En el artículo *algunas reflexiones sobre el concepto de información y sus implicaciones para el desarrollo de las ciencias de la información*, se define información de la siguiente manera "La información es el significado que otorgan las personas a las cosas. Los datos se perciben mediante los sentidos, estos los integran y generan la información necesaria para el conocimiento quien permite tomar decisiones…" (Goñi, 2000, p.203) Si esta información no se encuentra en un lugar donde nuestros sentidos puedan captarlos o si se encuentra de una manera que no podamos decodificar y analizar es una información prácticamente perdida.

2.2.2.1.- Protección-preservación-conservación

Muchas veces cuando se habla de protección tiende a confundirse la preservación con la conservación incluso llegando a verlos como sinónimos, para eliminar cualquier duda veamos algunas definiciones.

Protección: Son las acciones con el objetivo de resguardar o defender algo, evitando cambios en el estado inicial o actual de un ente o sistema en todas las formas perceptibles físicas o simbólicas. Podríamos decir que es aquello que puede evitar directamente una alteración del estado natural de algo ya sea tangible o intangible. (Este concepto es de elaboración propia, basado en la investigación del alcance del término en diferentes diccionarios y una previa experiencia del estudio de la teoría de sistemas)

Protección de datos: "Operaciones destinadas a resguardar los dígitos binarios que constituyen los objetos digitales de pérdidas o de modificaciones no autorizadas**." (**Biblioteca Nacional de Australia, 2003, p.165)

Una característica de la protección de la información que debemos tomar en cuenta siempre es que la protección de la información tiene dos vertientes, la protección de la información basada en el acceso a la información ya sea en materia de privacidad y confidencialidad o en cuanto a la capacidad tecnológica del soporte y la capacidad de decodificación de esa información (herramientas e idiomas).

Por otro lado tenemos la protección que se le da al soporte para lograr su conservación a través del tiempo

Preservación: Comprende todas las actividades económicas y administrativas que incluyen el depósito y la instalación de los materiales, la formación del personal, los planes de acción, los métodos y las técnicas referentes a la preservación de los materiales de archivos y bibliotecas y a la información contenida en los mismos. (Girón, 1988, p.1)

Preservación es: "…la organización y programación de toda clase de actividades relacionadas con la conservación de las colecciones en general…" (COMMA, 2001, p.59 c.p Calderón, 2009, p.3)

Conservación: Comprende los planes y practicas específicas, relativos a la protección de los materiales de archivos y bibliotecas frente al deterioro, daños y abandono, incluyendo los métodos y técnicas desarrollados por el personal técnico. (Girón, 1988, p.1)

Conservación es: "… el conjunto de operaciones que tienen por objeto prolongar la vida de un ente material, merced de la previsión del daño o la corrección del deterioro" (Viñas, 1988 p.2 c.p Calderón, 2009, p.2)

La diferencia entre preservación y conservación es que la conservación son las acciones para prevenir o corregir el daño, es una acción que implica una relación directa con el objeto o material a conservar para que este perdure en el tiempo. La preservación son los planes,

estrategias y manejo de recursos con la finalidad de crear o mejorar las acciones de conservación.

2.3.-Preservacion de lo analógico a largo plazo.

Más allá de los elementos de protección y preservación tradicionales e intuitivos para los soportes analógicos se trabajó con lo que podríamos decir que es el movimiento precursor de la digitalización, revolucionando a su vez aspectos como almacenamiento, durabilidad y movilidad de grandes cantidades de información.

Microfilmación: la preservación de la información en el pasado

-¿Qué es microfilmación?

La microfilmación también es llamada microfotografía, consiste en la reducción de imágenes a una escala tan pequeña que no puede ser leída sin asistencia óptica. Esta increíble compresión fotográfica usualmente ahorra un noventa por ciento de espacio, no debe confundirse con la fotomicrografía (usa lentes microscópicos para crear imágenes más grandes). La microfilmación es una de las prácticas más comunes en la reproducción de documentos, con el avance de la reproducción de documentos, la función de las bibliotecas no se restringe solo a la clasificación y al manejo de material impreso, el resguardo de microfilmaciones fue un factor importante en las ciencias de la información particularmente donde la reproducción era esencial para la preservación de la información.

La preservación de documentos raros y en deterioro es uno de los fines más importantes de la microfilmación, no es su forma física sino en su contenido intelectual; si bien los procesos de microfilmación se conocen desde hace más de 150 años no fue sino después de la segunda Guerra mundial que el uso de los microfilm se volvió muy popular como técnica de reproducción, en el caso de documentos importantes que podían dañarse por su uso constante se creaba una copia en microfilm y se resguardaba aparte, de necesitar el documento se hacía una reproducción de ese microfilm. El microfilm dado su material tiene una durabilidad mayor al papel si se cuida adecuadamente.

"Solo las películas de sales de plata en una base de poliéster con un resguardo adecuado de acuerdo a los estándares existentes se ha comprobado que pueden durar más de 1.000 años." (Dodson, 2001, p.1)[2]

-Microfilmación de 1920 a 1990.

En el año 1920 se da el primer uso práctico comercial a manos de un banquero Neoyorkino de nombre George McCarthy al que se le otorgó una patente en 1925 para su máquina Checkograph diseñada para hacer copias de todos los registros bancarios. En 1928 Eastman Kodak compro el invento de McCarthy y lo comercializo bajo la división "Kodak's Recordak". (Kodak, s/f, p.1)

En 1935 Recordak ahora con una cámara de microfilm de 35 mm expandió su mercado y comenzó a filmar y publicar el "New York Times" en microfilm; para 1938 por dos eventos particulares se aceleró el uso de microformas para preservación de archivos en bibliotecas e institutos Estadounidenses la primera, el rápido deterioro de los periódicos impresos y la dificultad de su resguardo por su material y dimensiones y segundo dado a que la biblioteca de la Universidad de Harvard comenzó su "Foreign Newspaper Project" (Proyecto periódico extranjero) que sigue vigente al día de hoy (Lamson, 2015, p.34); ese mismo año se fundó la University Microfilm Inc. (U.M.I.) ahora conocida como ProQuest a manos de Eugene Power. (Proquest, s/f, p.1)

Durante la segunda guerra mundial la microfotografía era usada extensivamente para espionaje y para correo militar regular, las cartas que iban de un continente a otro eran enviadas en microfilm, la guerra también trajo consigo destrucción de muchos registros de la civilización lo que aumento la urgencia de recaudar todos los documentos archivos y colecciones en microfilms para evitar la mayor pérdida de información posible.

Después de la guerra la idea de usar microformas para sistemas de información activos y solo para preservación de material fue propuesta, previendo que las bibliotecas utilizarían las microformas como fuentes de información y como medio de almacenamiento. Al obtener

[2] only silver halide film on a polyester base, processed and stored in accordance with the existing standards, has been proven to be capable of lasting more than 1,000 years

mayor financiamiento y mejor tecnología a finales de los años 50 y los años 60 impulso a los profesionales de la información a expandir sus actividades en el área de las microformas. (Southern Regional Library Facility [SRLF], s/f, p.1)

Por el boom de la información en los años 70 las bibliotecas e instituciones se vieron forzadas a usar las microformas como una alternativa ante los voluminosos medios impresos, el disponer de microfilms de mejor calidad, mejores lectores, impresores y la llegada de lectores portátiles hizo que fuera una opción más económica.

En las décadas de los 80 y 90 muchas de las microformas eran generadas por computadora y eran usados para catálogos, registros de compañías de seguro, registros de hospitales, listas telefónicas, registro de patentes y catálogos de bibliotecas; la permanencia de los microfilm para muchas bibliotecas e instituciones no solo era como una medida económica sino como una cuestión de preservación de la información. (Association for Library Collections & Technical Services [ALCTS], 2013, p.1)

2.3.1.-De lo análogo a lo digital

Lo digital es aquello representado por bits (ceros y unos), es lo que "lee" o procesa una computadora como secuencias de bits que le dan un significado, pero siempre requeriremos de un decodificador para recuperar esa información, en el caso de imágenes o documentos escritos un monitor, en caso de sonidos las cornetas y el uso de ambos para elementos multimedia como videos con sonido.

Digitalización

Al hablar de digitalización hablamos del proceso mediante el cual transformamos algo de origen analógico (físico) en algo digital (elemento formado por conjuntos de unidades binarias) que podemos manipular informáticamente.

¿Cómo funciona un escáner? Los escáneres funcionan con sensores de imagen, el más comercial y usado en la mayoría de los escáneres destinados a documentación se encuentra el

CCD (Charge Coupled Device) en el cual se ilumina la imagen a digitalizar con un foco de luz que es redirigida a los sensores CCD que transforman la luz recibida en señales eléctricas que luego usando un conversor analógico-digital se vuelven señales digitales que luego son transformadas en bits que el computador procesa.

La resolución óptica de un escáner resulta del número de los elementos en la línea CCD y del ancho de la imagen.

Grabación de sonido: muy común desde hace años, al proceso de transformar sonido analógico a secuencias binarias se le llama muestreo proveniente del inglés sampling, el método más común es mediante el uso de un micrófono que a través de una membrana registra las vibraciones sonoras; en algunos casos se usa software y hardware especializado para pasar de otros formatos analógicos (casete, vinilo, cintas magnéticas)

Lo intencionalmente digital

Con el volumen de documentos que se maneja en la actualidad se revierte la tendencia de tener un documento físico y procurar su digitalización a la creación y uso de documentos creados en el computador para su posterior disposición física de ser requerida, incluso en términos legales ya muchos países usan el llamado “gobierno electrónico” y dan validez legal a documentos electrónicos que posean firmas electrónicas (normalmente otorgados por empresas de certificados digitales admitidas por el estado) (SUSCERTE, 2009), por lo que cada día que pasa es más necesario crear lineamientos para la protección de la información digital.

Fragilidad digital

Como se mencionó anteriormente aun cuando el entorno digital nos ofrezca muchas ventajas es muy frágil, no solo por depender del hardware para su almacenamiento sino que también dependemos del hardware y el software para su lectura y para su posterior reproducción (en caso de ser necesaria), el avance exponencial de la tecnología también atropella al resguardo de la información si no nos cuidamos, el cambio de sistemas operativos, nuevas versiones de software de lectura o edición de archivos no siempre son mejoradas con

una propuesta de compatibilidad con sus antecesores aun cuando su funcionalidad sea 90% similar.

> …Afortunadamente, cada vez hay más iniciativas y más proyectos dedicados al tema…Por supuesto en paralelo, la fragilidad digital nos obliga a los documentalistas a extremar las precauciones en todos los proyectos en los que intervengamos relacionados con información digital. De este modo, junto a aspectos como la organización hemos de tener presente siempre el de la preservación. (Codina, 2001, p.6)

Reproductividad

Hablar de la reproductividad de la información no es más que la cualidad que posee la información de ser replicada para facilitar su acceso y prolongar su alcance, en la antigüedad era tarea de los escribas el reproducir los textos trabajando en conjunto con los iluminadores para crear un ejemplar, era posible crear copias de un ejemplar ya existente, pero cada trabajo era único y consumía una gran cantidad de tiempo; con la imprenta el tiempo de reproducción redujo mucho, pero la calidad del trabajo junto con ella (comparándolo con libros trabajados en vitela con oro y pigmentos naturales)y hoy día en la era digital, se pueden crear y reproducir documentos de una manera extraordinariamente rápida y que tengan un impacto visual de gran calidad.

Digital

La capacidad de un archivo digital en replicarse es uno de sus fuertes, la sencillez y rapidez con la que un archivo digital puede duplicarse dentro de un computador con conexión SATA es asombrosa ya que cuenta con transferencias de archivos con velocidades de hasta de 150mb por lo que un archivo de texto promedio de 200 páginas que pese cerca de 2mb se copiaría en cuestión de microsegundos. (LSI, 2014, p.1)

Dentro de las estrategias comunes para protección de la información digital es el poseer varias copias de un mismo documento en distintos lugares, cualquier estudiante puede sentirse identificado con el siguiente proceso: crear un documento en su computadora de escritorio,

enviársela a sí mismo por correo electrónico donde queda una copia y bajarlo en una laptop o en un computador ajeno con acceso a internet para luego copiarlo en su pen-drive y llevarlo a una presentación. Con lo que ya dispone de 4 lugares distintos de donde disponer de tu información en caso de perderla.

De lo digital a lo analógico

Con anterioridad hablamos de la necesidad de un decodificador para recuperar la información digital, aun cuando escaneemos una imagen o un documento, grabemos audio o video, siempre necesitaremos de algo que nos devuelva una información analógica para nuestra comprensión, para poder visualizar una fotografía o algún documento escrito necesitaremos siempre de un monitor o de una impresora que lo transmita a papel, para grabaciones de voz o de instrumentos debemos hacer uso de auriculares, cornetas, y en caso de la medición de frecuencias monitor e impresoras.

2.4.- Preservación digital

Una vez vista la diferencia entre preservación y conservación debemos saber cómo se une el concepto de preservación con el entorno digital. ”Consiste en mantener la capacidad de presentar los elementos esenciales de objetos digitales auténticos. Debe hacer frente a peligros que pueden amenazar cualquiera de los elementos del objeto digital: material, lógico, conceptual y esencial.” (Carrión, 2007, p.67) un hecho importante a considerar en la preservación digital es el siguiente:

Para entidades de información digital… no hay una definición aceptada de preservación digital que asegure salvar todos los aspectos de esas entidades. Al escoger un método de preservación digital en particular, determinamos que aspectos de esa entidad son preservados y cuáles serán sacrificados. (Traducción propia)[3]

[3] For digital informational entities ... There is no accepted definition of digital preservation that ensures saving all aspects of such entities. By choosing a particular digital preservation method, we determine which aspects of such entities will be preserved and which ones will be sacrificed. (Rothenberg, 1995, p.55).

Dada la computabilidad de la información digital el verdadero reto de su preservación no recae en tener disponible un objeto analógico que contenga esa información digital “La mayor amenaza para la continuidad digital es la desaparición de los medios de acceso. No puede decirse que se han conservado los objetos digitales si, al ya no existir los medios de acceso, resulta imposible utilizarlos.” (Biblioteca Nacional de Australia, 2003, p.37).

La copia o reproducción de datos que componen esa información digital legible para el humano es increíblemente rápida y sencilla, su capacidad de transmisión en relación, cantidad de información y tiempo de transmisión es inigualable y en cuanto a su almacenamiento en relación de espacio físico y cantidad de información es abrumadora. Por esas razones podemos afirmar que hoy día, la accesibilidad de la información digital es casi inmejorable dado a que los discos duros convencionales copian sectores de datos a velocidades hasta 7000 revoluciones por minuto y los procesadores actuales de alto rendimiento pueden procesar cerca de 72 mil millones de operaciones aritméticas por segundo. (UNOCERO, 2008, p.1)

La UNESCO además de mencionar algunas de las ventajas del patrimonio digital nos presenta los problemas para mantener utilizable y disponible ese patrimonio digital, para lo cual plantean un proyecto de carta de la UNESCO donde nos habla del patrimonio digital, su acceso, su riesgo de pérdida, continuidad digital hasta llegar a desarrollar la protección del patrimonio digital. (Biblioteca Nacional de Australia, 2003, p.159)

Allì hablan del cambio continuo de los formatos digitales y el problema que conlleva el avance rápido de la tecnología en la cual asume nuevas formas y formatos, llevándonos primero al hecho indiscutible que en las bibliotecas se debe resguardar también la información digital, segundo: el cambio en la tecnología es tan rápido que su obsolescencia en muchos casos puede ser menor a la mitad de una generación (según la genealogía una generación es cada 25 años) por lo que deben crearse métodos de preservación para medios digitales, uno de los mayores problemas no es donde se resguarda la información digital en sí, sino la del medio donde este se reproduce, para lo cual se plantean la migración de datos a formatos más nuevos y a la emulación de sistemas, refiriéndose al proceso de recrear artificialmente el ambiente de un sistema operativo en otro, así el software diseñado para ejecutarse en un sistema más antiguo pueda ser usado en uno más nuevo.

En su conclusión determinan que dado los problemas de estandarización de metadatos, de derechos de autor y propiedad intelectual de sistemas operativos, la migración de datos o la emulación de sistemas podrían no ser viables para el momento, desde ese entonces plantearon una meta: crear un sistema de preservación a largo plazo basado en el estándar internacional OAIS para diseñar esquemas para metadatos.

Hilde van Wijngaarden (2008) al igual que la NDL de Japón (2006) proponen el uso de estrategias como: la migración y emulación considerando estudiar cómo puede afectar cualquiera de los siguientes cinco aspectos en un archivo digital, los cinco aspectos se presentan a continuación:

Contenido: es la parte invariable que debe ser conservada en su codificación y estructura originales.

Contexto: "Hay que aclarar que el contexto se refiere a los diferentes aspectos que afectan al documento, por ejemplo quien firma, la relación que tiene con otros documentos… la función que ejerce" (Marcos, 1999, p.2)

Estructura: Las reglas de representación acorde a la cual el contenido de un documento, su contexto administrativo, documental y su autoría son comunicados. (Van Der Hoeven; Van Wijngaarden, 2005)

Apariencia: En documentos digitales incluye todo aspecto que influya en su diseño visual, para textos la fuente: el color del texto, anexos, para fotografías: color, contraste, resolución, tamaño, entre otros. (Van Der Hoeven, et al, 2005)

Comportamiento: El comportamiento de un objeto digital se refiere a los procesos o acciones insertadas en su código que operan sobre un estado del objeto. (Van Der Hoeven, et al, 2005)

Dentro de la preservación digital debemos tener en cuenta varios aspectos para lograr elaborar una estrategia eficiente que logre preservar el acervo digital, a continuación se presentan aspectos de ocurrencia propia basada en mi experiencia:

-Toda información digital debe estar contenida en un ambiente físico y por esa razón debemos disponer de un lugar seguro para el servidor, entendiéndolo como el hardware que dispone de elementos suficientes para almacenar y procesar datos e instrucciones que reproducen un archivo digital para que sea legible a nivel humano.

-Al igual que con la información analógica, debemos dar prioridad a los materiales para su preservación, aun cuando el espacio físico que ocupa un servidor no es mucho y el que ocupa la información almacenada en ellos es casi nula el espacio disponible en un servidor es finito "Reconocer que no es realista tratar de preservar todo y que hay que seleccionar el material que debe ser preservado." (Biblioteca Nacional de Australia, 2003, p.37).

-Conservar la información digital evitando cualquier cambio en los datos, ya sea a nivel de estructura o de contenido.

-Después de su almacenamiento en el servidor hacer uso de software de base de datos, metadatos estructurados que mejoren la accesibilidad de la información.

-Hacer uso de medios apropiados que nos garanticen en mayor medida el acceso a la información a través del tiempo intentando evadir la obsolescencia tecnológica.

-Crear planes de preservación digital basados en estudios previos de la situación del centro de información en cuanto a su material digital.

-Revisar rigurosamente la seguridad de las redes de las que dispongan los servidores, con mayor medida si el servidor tiene acceso externo.

-Trabajar en conjunto con editoriales, autores e instituciones relacionadas con el manejo de la información para crear y aplicar normativas que extiendan la vida útil de la tecnología para acceso y reproducción de información digital.

2.4.1.- Metadatos para la preservación digital.

Todo profesional de la información en la actualidad seguramente está familiarizado con el termino *metadatos*, viéndolo muchas veces como simples *datos sobre datos*, sin embargo incluso dentro de los metadatos hay una tipología que puede llegar a ser bastante extensa.

Existe un grupo de trabajo internacional que es patrocinado por el Online Computer Library Center (OCLC) y el Research Libraries Group (RLG) denominado PREMIS (por las siglas de Preservation Metadata: Implementation Strategies) y trabajan enfocados en metadatos de preservación, La Biblioteca Nacional de España define los metadatos de preservación como:" la información que utiliza un repositorio para soportar el proceso de preservación digital". (PREMIS, 2010, p.10)

Dado a que la información digital es fácilmente alterable, los metadatos de preservación proporcionan herramientas suficientes a los profesionales de la información para hacer un análisis sobre la integridad de un documento digital y saber si fue violentada. Conocer las ventajas y posibles usos que ofrecen los metadatos de preservación sin duda es un paso necesario en las actividades bibliotecológicas de la nueva era digital.

Dentro de las características que poseen los metadatos de preservación tenemos:

-En ellos se registra el tipo y la edad del soporte de almacenamiento y las fechas en las que se refrescaron los ficheros por última vez. (PREMIS, 2010, p.13)

-La comparación de los metadatos de preservación en dos momentos distintos puede expresar la posibilidad de que un archivo haya cambiado, por más mínimo que sea el cambio. (PREMIS, 2010, p.208)

-En los metadatos de preservación podemos encontrar firmas digitales, o información del origen digital de un archivo e incluso un historial de cambios autorizados. (PREMIS, 2010, p.107)

-Pueden contener inhibidores que prohíban la modificación de un archivo digital o deje un rastro al ser modificado sin una autorización previa. (PREMIS, 2010, p.223)

CAPÍTULO III – Marco metodológico

3.1.- Tipo de investigación:

El tipo de investigación es documental expositiva ya que este tipo de investigación "Es la panorámica de la información relevante que se encuentra en diversas fuentes documentales… sobre un tema específico"(Jiménez, 2013, p.12) . Esta investigación establece lineamientos para proponer soluciones a la pérdida de información digital, para ello, en este proyecto se revisó el paradigma de la bibliotecología en cuanto a la preservación de la información digital, se analizaron los factores de preservación, se identificaron los métodos más eficientes para ello y en base a eso se dan las directrices que constituyen los lineamientos para lograr la preservación de la información digital.

3.2.- Diseño de investigación:

De acuerdo a los parámetros que se toman en cuenta para catalogar el diseño de una investigación, el presente trabajo especial de grado se caracteriza por ser del tipo no experimental ya que no se manipulan variables, transeccional porque se recolectan datos en un solo periodo de tiempo, descriptiva porque se busca describir propiedades de fenómenos o sujetos a ser analizados y documental porque parte de la información se obtendrá de documentos escritos anteriormente. (Hernández, Fernández y Baptista, 2003)

Por otra parte tenemos que la investigación documental se define como parte fundamental de un trabajo de investigación, queriendo decir con esto que se transforma en una estrategia donde el investigador observa y reflexiona sistemáticamente sobre realidades teóricas o no, usando para ello diferentes tipos de documentos.

3.3.- Población-muestra:

Ya que la población es una representación del universo de estudio y la muestra un subgrupo de la población (Hernández, et al, 2003), La muestra de la investigación abordó el estudio de los factores de preservación de la información en todas sus formas accesibles, análogas y virtuales que puedan ser preservadas en un ambiente digital.

3.4.- Técnica e instrumentos de recolección de datos:

La recolección de datos para esta investigación fue el análisis de contenido que "Es una técnica para estudiar y analizar la comunicación de una manera objetiva, sistemática y cuantitativa" (Berelson, 1952, c.p Hernandez, et al, 2003, p.301) que "puede ser aplicado virtualmente a cualquier forma de comunicación" (Hernandez, et al, 2003, p.301), es decir las técnicas de síntesis y análisis. Se aplicó esta técnica ya que se procedió a revisar, leer y analizar libros, revistas, documentos, de Internet y cualquier otro tipo de fuentes documentales para reunir la información necesaria para realizar la investigación.

3.5.- Técnica de análisis y representación de los datos:

Ya que se necesitan datos descriptivos para ahondar y presentar los lineamientos a proponer, la técnica de análisis a usar en esta investigación es el análisis cualitativo de contenido.

> El análisis cualitativo de contenido se define a sí mismo dentro de este marco de trabajo como una aproximación empírica, de análisis metodológicamente controlado de textos al interior de sus contextos de comunicación, siguiendo reglas analíticas de contenido y modelos paso a paso, sin cuantificación de por medio (Mayring, 2000, c.p en Cáceres, 2003, p.56).

CAPÍTULO IV – Análisis contextual

4.1- Paradigmas

Para crear de manera objetiva unos lineamientos para la protección de la información digital, debemos describir el paradigma de la bibliotecología con los rasgos característicos que han predominado en el desempeño de nuestras tareas como profesionales de la información. De esta manera, podremos ver las posibles debilidades que todavía posee la bibliotecología en términos de protección de la información.

Cada momento en la historia es distinto y al igual que muchas otras disciplinas, la bibliotecología ha pasado por grandes cambios de tipo teórico, metodológico y conceptual. Pero, su objetivo principal se mantiene, aun cuando lo redactemos de distintas formas: proteger la información.

Podríamos decir que en la edad de piedra desde los primeros registros que datan del periodo paleolítico superior, sin saberlo, el mismo neandertal que creó una pintura rupestre en su cueva también se volvió custodio de esa información. Esto lo hizo al proteger dicha cueva contra cualquier animal invasor o incluso de otros de su especie, aun cuando claramente su prioridad era la supervivencia más básica, quizás hasta el tercer escalón en la pirámide de Maslow. El escriba egipcio, era el encargado de contar, clasificar y registrar las transacciones que realizaba su pueblo, y el amanuense o copista en la edad media dentro de las escuelas monacales hacía trabajo de editor y trabajaba junto a los iluminadores para crear libros con un acabado increíble

Una de las características en común de los referidos en el párrafo anterior, es que quien crea los registros era a su vez el custodio de la información, cosa que cambiaría drásticamente

Con la llegada de la imprenta moderna de Gutenberg, aproximadamente en 1440, a pesar de que significó un gran avance en el tema de distribución y acceso a la información, también ocasionó un problema. Este fue que para acceder a la información de distintos ámbitos o buscar sólo la información que era de interés para una persona, se requería mucho tiempo por el hecho de que debía recurrir a copistas o a algún artista xilógrafo puesto que el coste del papel en el siglo XII era todavía mucho mayor al del papiro. (Velduque, 2011)

Si bien es cierto que dentro de los conceptos de conocimiento e información, existen autores con diferencias o quizás ambigüedades poco claras, a medida que avanzamos y cambia nuestro entorno informacional, se irán transformando los conceptos. Por ello debemos hablar de 3 de los paradigmas de la bibliotecología con más fuerza

4.1.1.- El paradigma físico:

Al leer los trabajos de Ania Hernandez, Rafael Capurro, Germán Castaño, Francisco García y otros autores se hace notable que todos ven como responsables del paradigma físico (moderno) a dos personas destacadas: Claude Shannon y Warren Weaver. Ellos crearon un modelo de comunicación y de recuperación de información en bases estadísticas y sistematizando elementos que de una u otra manera están dentro del proceso de comunicación. Si bien, esto fue un gran avance y, aún representa un enfoque productivo. El paso del tiempo ha llevado este concepto tal como se usaba a parecer un poco incompleto.

Ciertamente podría decirse que toda información tiene una representación en el mundo analógico, un soporte o ente físico en algún lugar, mediante el cual tomamos la información (viendo la información como la capacidad de recoger datos de nuestro entorno por cualquiera de nuestros cinco sentidos) para darle usos que cumplan nuestras metas.

En 1966, cuando se daban los primeros pasos en las técnicas de recuperación de información en medios electrónicos, se publicó el *Aslib-Canfield research project* (iniciado en 1957). Así pues, el avance en materia de indización con este proyecto fue un éxito como podemos observar descrito en las consideraciones generales de éste.

> Con las pruebas del índice de literatura metalúrgica de la Western Reserve University, se mostró que podría hacerse una evaluación de un sistema operacional con comparativamente poco esfuerzo y usando solo una pequeña muestra de la colección. Desde ese momento se han realizado mejoras en la metodología, y la experiencia muestra en lo que respecta a mejoras todavía son necesarias, pero los

> métodos generales probados por primera vez en 1962 fueron usados con éxito en un número de aplicaciones diferentes (Traducción propia).[4]

Bajo este paradigma han surgido muchas de las herramientas imprescindibles en el manejo de información como: tesauros, metadatos, palabras claves, sistemas de búsqueda, organización de material por tema, indización, procesos técnicos, entre otras.

A mi consideración este es el paradigma más arraigado o con mayor alcance en la bibliotecología dado a que el uso las herramientas propias de este paradigma forma la parte más notable para el público en cuanto al servicio de referencia prestado en muchas instituciones actualmente, eso y que su enfoque en la protección del soporte crea un vínculo con la etapa conservacionista de la bibliotecología.

Con el paso del tiempo y viendo los riesgos a los que se exponen los documentos, se han creado normativas para la protección y recuperación de los soportes que contienen la información por parte de instituciones internacionales como la IFLA Z39.50 en recuperación de información, las normas UNESCO de protección y promoción de la cultura (UNESCO 2013) y la serie ISO 27000 en protección de la información (ISO27000, 2005). Siguiendo como ejemplo estos estándares internacionales la Biblioteca nacional de Venezuela ha creado sus propias normas como las CONSERVAPLAN en materia de protección de los soportes ante el medio ambiente (Biblioteca Nacional de Venezuela, 1998), enfocadas en la preservación y restauración de documentos con tópicos como:

-el manejo adecuado de un libro.

-el uso de tipos de materiales para la estantería.

[4] "With the test of the index of metallurgical literature of Western Reserve University, it was shown that an evaluation could be made of an operational system with comparatively little effort and by using only a small sample of the collection. Since that time improvements have been made in the methodology, and experience has shown in what respects improvements are still necessary, but the general methods first tried in 1962 have been successfully used in a number of different applications."

-regulaciones del medio donde se pretenda almacenar los ejemplares (localización dentro del edificio)

-prevenciones contra incendios, inundaciones y factores ambientales (humedad, luz, temperatura).

-prevenciones contra plagas.

-prevenciones contra factores humanos.

-evaluación de ejemplares.

-políticas de traslado de materiales.

-especificación de estándares para protectores y cubiertas.

-métodos de restauración.

-duplicación de material.

En este paradigma es muy pequeña la separación entre las ideas de: documento e información. Si bien como mencionamos toda información posee algún ente analógico no debemos concluir que sólo los escritos en cualquiera de sus formas integran el universo de la información. Esta no está ligada únicamente a los documentos sino a todo lo que existe y en la aplicación práctica del paradigma físico existe mucha información que se pierde por no considerar una protección más allá del soporte.

En el mundo digital muchas medidas de protección físicas podrían también ser aplicadas o adaptadas a los entornos donde se mantiene la información digital, servidores, memorias USB, discos duros, memorias SD, la nube o cualquiera de sus formas, que también tienen sus propias ventajas y desventajas en cuanto a la durabilidad del material, resistencias al medio ambiente como la humedad, contaminación del aire, temperatura, vulnerabilidad ante daño físico premeditado (vandalismo) o no premeditado como inundaciones, incendios y de igual forma requerirán planes de contingencia para dichas ocasiones.

Con la era digital y una distribución de la información mucho más acelerada y diversa debemos ser un poco más inclusivos con los métodos de protección de la información e ir un poco más allá para ver la información como algo fuera del soporte, en el paradigma cognitivo se plantea el *tercer mundo* (Popper, 1978) y en el paradigma social buscan incluir al humano como parte del principio por el cual se genera la información pero ambos paradigmas están claros en un punto: la información no es sólo el documento donde se encuentra.

4.1.2.- El paradigma cognitivo:

En el paradigma físico de la Bibliotecología que es el más tradicionalista la relación directa de libro-información ha cambiado un poco, una evidencia de esto la encontramos dentro del "Tratado de documentación" publicado por Otlet en 1934 podemos evidenciar que:

> En esta obra Otlet habla del libro y del documento pues, atento al desarrollo de su tiempo, infiere que el libro ya no sería el único contenedor de información y considera a los nuevos tipos de materiales que iban surgiendo: fotografías, diapositivas, fotocopias, películas de cine, programas de radio. Comenta entonces que el libro debía dejar paso a un concepto más amplio y universal, el documento. (García y Cárdenas, 2002, p24)

Por otro lado el paradigma cognitivo se enfoca en el conocimiento, pero planteando que el conocimiento existe en un lugar propio independiente que en el caso de Otlet y Lafontaine el conocimiento no está ligado a los documentos solamente.

> ...en las ideas de una bibliografía universal de Paul Otlet y Henri Lafontaine... está explícita la idea de distinguir entre los conocimientos y su fijación en documentos. La documentación y luego la ciencia de la información tienen que ver aparentemente en primer lugar con los portadores físicos del conocimiento, pero en realidad su finalidad es la recuperación de la información misma o sea del contenido de dichos portadores. (Capurro, 2007, p19)

En los planteamientos originales de Popper ese lugar propio donde se encuentra en conocimiento es el *mundo tres* o *tercer mundo* donde plantea que la existencia del conocimiento es independiente a la cognición humana. (Popper, 1978, p.153)

El no considerar dentro de este paradigma al hombre como ente cognitivo deja por fuera muchos aspectos de la bibliotecología como el trabajo del referencista, los procesos técnicos, podría decirse que incluso a los autores, en la definición del *tercer mundo* planteado por Popper, donde la información existe en otro plano en sí misma pero falta que la consigamos, tiene una lógica más de tipo utopía filosófica, bajo ese planteamiento podría decir cosas que si bien no son veraces tampoco podría considerarse una falacia, al decir "la máquina del tiempo puede existir, solo que no sabemos cómo hacerla" un simple planteamiento como ese crearía paradojas del tipo "si un árbol cae y no hay nadie presente, ¿hace ruido?" donde no tenemos suficiente información y, podría avalarse solo porque a alguien se le ha ocurrido pero no negada porque no es demostrable.

Dentro del mismo paradigma cognitivo hay quienes buscaron ligar ese tercer mundo con el potencial cognitivo de hombre, Kuhlthau lo denominó el principio de incertidumbre mientras que Belkin, Oddy y Brooks llamaron "Estado anómalo del conocimiento".(más conocido en inglés como Anomalous State of Knowledge por sus siglas ASK) donde buscan ese vínculo entre el conocimiento y el hombre bajo la premisa que la búsqueda de información se origina siempre por una necesidad cuando el estado cognitivo y contextual de un sujeto no es suficiente para afrontar un problema por ejemplo "*su estado anímico, sus creencias, los objetivos planteados, su grado de motivación o sus áreas de interés, entre otros.*" (Quesada, 2002, p108)

Existe una frase muy conocida "la información es poder" y desde tiempos antiguos eso es una realidad, el poder no era el documento, sino la información que allí se encontrase, en la información más simple puede estar la diferencia incluso entre la vida y la muerte, saber la posición del enemigo, si lloverá o no, la posición de una estrella en relación a otras, todo eso puede ser documentado, pero la información persiste y existe fuera de los documentos.

En el entorno digital la información que es creada igual tiene un lugar físico, pero al no ser legible por nosotros en su forma más básica, al no poder extraerlo de su núcleo sin computadores y software también tiende a ser menospreciado como entorno meramente cognitivo, el paradigma cognitivo podría trabajar en función de la información sin quitarle la importancia al soporte o al usuario, políticas de protección para la información a nivel intangible a un nivel donde intervenga tanto el soporte (porque al final todo tiene en algún lugar su entorno analógico) como el hombre como ente que: necesita, crea y administra información.

Gardner y Riviere (1991) consideran que el procesamiento de la información en su principio está unido a la visión racionalista de la filosofía dando mayor importancia a la información como proceso cognitivo creado por el hombre (ideas, conceptos, planes, o cualquier tipo de acción cognitiva) por encima de los documentos o registros que puedan existir durante el proceso del conocimiento.

> Dicho de otra manera, para los cognoscitivistas los comportamientos no son regulados por el medio externo, sino más bien por las representaciones que el sujeto ha elaborado o construido. Por tanto a diferencia del enfoque conductista, donde el sujeto está controlado por las contingencias ambientales, en este paradigma el sujeto es un ente activo, cuyas acciones dependen en gran parte por dichas representaciones o procesos internos que él ha elaborado como resultado de las relaciones previas con su entorno físico y social. Esto significa al mismo tiempo que el sujeto de conocimiento deja de ser una tabula rasa, que simplemente acumula por asociación impresiones sensoriales para ir conformando sus ideas sobre lo real. Por el contrario, el sujeto organiza tales representaciones dentro de su sistema cognitivo general, las cuales les sirven para sus posteriores interpretaciones de lo real. (Hernández, 1997, p 4-5)

En el paradigma cognitivo la protección de la información se enfoca más en el nivel jurídico en ámbitos de confidencialidad y autoría incluyendo detalles respecto a su distribución, acceso y uso. Para evitar la pérdida de información en el paradigma cognitivo lo mejor es incentivar la circulación de la información: por repetición a nivel cognitivo, por reproducción

a nivel físico y mejorando el acceso en ambos niveles, siempre en conformidad con las leyes establecidas para la protección de la confidencialidad y autoría.

4.1.3- El paradigma social:

En el paradigma social a diferencia del cognitivo se considera la importancia del hombre como punto central, al igual que Kuhlthau, Belkin, Oddy y Brooks la principal base para esa integración del hombre era la llamada "necesidad de información", Frohmann en su crítica del paradigma cognitivo describe la poca importancia de la actividad humana en la creación y manejo de información de la siguiente manera "el punto de vista cognitivo relega a los procesos sociales de producción, distribución, intercambio y consumo de información a un nivel numenal..." (Frohmann c.p Capurro, 2007,p20) refiriéndose al sentido que le dio Kant en que lo numenal (noúmenico) no creía que pudiera ser demostrado de manera racional o empírica.

> Es evidente también el valor del paradigma social, que posibilita la mayor cobertura de las investigaciones realizadas, ya que el paradigma físico excluye el sujeto cognoscente del proceso de recuperación de la información, y el paradigma cognitivo no es suficiente para suplir las demandas pragmático-sociales de un grupo de personas (Deliberali, 2011, p3)

El paradigma social "integra la perspectiva individualista e isolacionista del paradigma cognitivo dentro de un contexto social en el cual diferentes comunidades desarrollan sus criterios de selección y relevancia" (Capurro, 2003, c.p Deliberali, 2011, p3).

> El análisis de dominio de Hjorland es un intento de una teoría comprensiva que puede ser aplicada a las ciencias de la información. Su premisa principal es un conjunto de herramientas analíticas que pueden ser aplicadas en subgrupos o como un todo para estudiar los efectos de diferentes campos sociales, epistemológicos y culturales de las

> teorías de la ciencia de la información. En consecuencia esta organización es aplicada en relación a los diferentes dominios de los cuales emanan y son consumidos. En vez de estudiar al usuario en este caso el dominio o medio ambiente es el foco principal de la teoría. Los individuos son vistos como miembros de distintas culturas o dominios y su sistema documental subsecuente. (Traducción propia)[5]

La información en el paradigma social es vista como:

> "Pues la información -ese bien de consumo tan valorado que mueve los engranajes de la post-moderna 'Sociedad del Conocimiento'- es herencia y producto cultural humano, perteneciente a toda la especie, y debería ser de libre disfrute. Mediante su empleo equilibrado, igualitario y solidario, los grupos humanos pueden elegir, y tal elección puede permitirles bienestar, desarrollo, educación, pensamiento independiente y opinión crítica. Algo peligroso para los sistemas hegemónicos, que verían peligrar su poder y su influencia." (Civallero, 2004, c.p Montenegro y Repetto, 2006, p2)

Con esto observamos que en el paradigma social la información se ve como algo producido por el hombre, para el hombre y necesario para lograr mantener el ciclo del conocimiento de necesidad de información, producción de información y uso de esa información.

"La información es tratada desde una perspectiva amplia que involucra, además de los mensajes (paradigma físico), que son procesados a un nivel cognitivo (paradigma cognitivo), un contexto -situación, tarea, problema-, motivaciones e intencionalidad" (Saracevic, 1999, citado en Vega, Molina & Linares, 2009)

---

[5] Hjørland's Domain Analysis is an attempt at a comprehensive theory that can be applied to Information Science. Its main premise is a set of analytical tools that can be applied in subsets or as a whole to in order to study the effects of different social, epistemological, and cultural fields on the theories of Information Science. Thus organization is applied in relation to the different domains from which it emanates and is consumed. Rather than studying the user in this case, the domain or environment is the main focus of the theory. Individuals are seen as members of distinct cultures or domains and their subsequent document systems

La protección de la información en el ámbito social es más fuerte en tema de accesibilidad dado a que muchos grupos políticos, económicos, creencias generan diversa información que posiblemente otros grupos esperan no sea divulgada y en ocasiones se hace uso de ventajas políticas, económicas o diversas medidas de presión para evitar el libre acceso a toda la información existente.

> "El poder de la información y, sobre todo, el que contienen y representan los soportes escritos, han sido controlados, manejados e influidos a lo largo de toda la historia humana por los poderes e ideologías dominantes. El actual paradigma de 'Sociedad de la Información' perpetúa tales políticas, generando profundos desequilibrios en el libre acceso al saber, y por ende, en las posibilidades de desarrollo y progreso de las sociedades humanas." (Civallero, 2004, citado en Montenegro y Repetto, 2006, p72)

Unos de los esfuerzos más reconocidos en materia de libre acceso de la información y libertad de expresión podemos encontrarlo en el artículo 19 de la Declaración Universal de los Derechos Humanos

> Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

En el caso de Venezuela podemos apreciar los esfuerzos en materia de acceso y libertad de expresión en los artículos 28 y 143 de la Constitución Nacional

4.1.4- Paradigma actual de la Bibliotecología.

En el paradigma social, se habla de la necesidad de información, en el paradigma cognitivo se habla del "information retrieval" o recuperación de información y en el paradigma físico ya se tienen herramientas para ejecutar esa recuperación de información que ayuda a resolver esa necesidad, pero el paradigma actual enfocado en el paradigma social debe encontrar la forma de unir por completo estos tres paradigmas ya que primero: sin el

hombre el paradigma social no tiene razón de ser dado a que sin un sujeto no existiría demanda de información, segundo: la recuperación de información a nivel cognitivo no existiría y los procesos tradicionales de recuperación de información no podrían ser ejecutados ya que se requiere de ciertos procedimientos mecánicos y cognitivos para recuperar la información deseada en su forma física.

Por más automatizado que sea siempre un sistema, en algún punto de ese sistema estará incluido el hombre.

En la actualidad hay que considerar que la información va más allá del documento y debemos operar en función de recuperarla admitiendo que toda información que existe posee un entorno analógico sin importar que la forma de acceso sea desde un entorno digital o no, la capacidad cognitiva del ser humano impulsada por la necesidad de información y mediante la investigación nos da la capacidad de extraer la información del llamado tercer mundo, pero dada la gran cantidad de información que creamos y distribuimos necesitamos de sistemas de gestión de información para conseguir la información pertinente de acuerdo a nuestra necesidad actual.

Dentro de las características que debemos considerar que posee la información en la actualidad están:

-Somos capaces de encontrar información en cualquier cosa que podamos percibir mediante nuestros 5 sentidos de forma asistida o no, las herramientas y registros nos dan una información más específica sobre un hecho, más no significa que sin ese registro el hecho no exista, un ejemplo: al encender una luz, y observar su intensidad podemos saber si es suficiente o no para la lectura aun cuando no dispongamos de un luxómetro que nos dé una lectura de 200 a 300 lux óptimos para una sala de lectura, podría decirse que *primero hecho, luego registro*.

-Toda información tiene un aspecto analógico: En el caso de lo que conocemos como información digital o entorno virtual debemos recordar que dependen de un hardware donde se encuentra la información en una forma que no podemos decodificar por medio de nuestros

5 sentidos de manera convencional y son transmitidos desde su posición original por cable y/o por medios inalámbricos.

-Aun cuando concuerdo con la existencia del *tercer mundo* planteado por Popper, el único método lógico para extraer información de ese *tercer mundo* es mediante el uso de la capacidad cognitiva del ser humano por lo cual no debe ser descartado del proceso de recuperación de información.

-con la gran cantidad de información que podemos encontrar, ya sea de bases confiables o no e incluyendo información repetida en diferentes lugares de la web que no poseen una cita que nos ayude a localizar el documento original deberíamos incluir un aspecto que basándonos en la teoría de Shannon deberíamos considerar hoy día para la información digital,

-El número de ***selecciones disponibles*** menos las ***selecciones útiles*** podríamos llamarlo ***Ruido***

-El número de ***selecciones útiles*** menos las ***selecciones no decodificables*** podríamos llamarlo ***información conveniente***

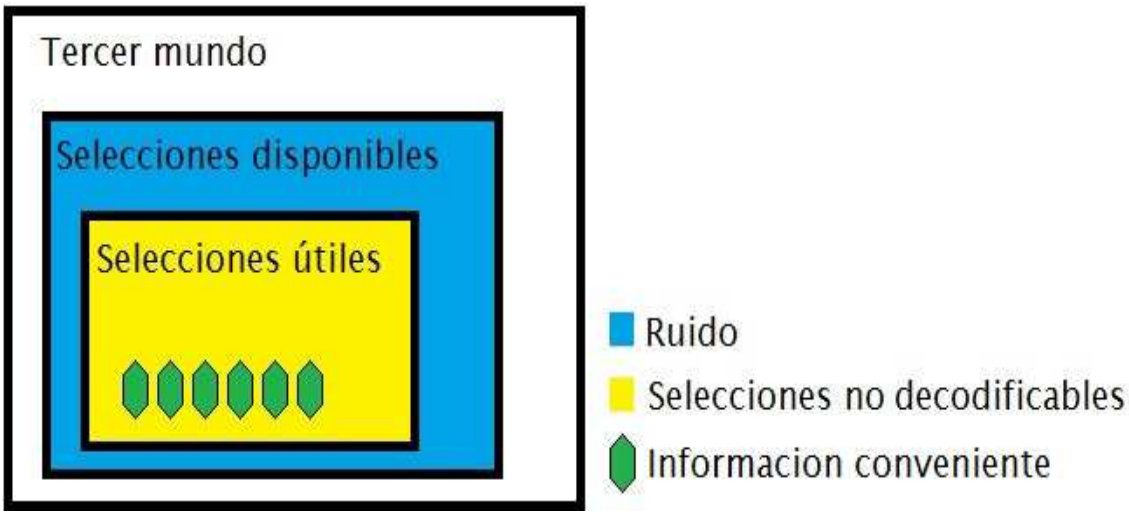


Figura 1. Explicación grafica de la información conveniente (elaboración propia)

-toda selección disponible debe encontrarse procesada (catalogado, clasificado, indizado, etc.) para lograr su recuperación mediante un sistema de búsqueda ya sea especializado en un tipo

de información o no. Esta consideración seria enfocada a lograr recuperar la mayor cantidad de información conveniente (definido arriba)

Otro factor no incluido en los paradigmas anteriores de forma directa es el considerar la información no sólo como aquellos datos con algún significado y utilidad encontrados en un documento sino también como un ente transmisible mediante la comunicación de persona a persona, en una sola palabra, considerar la *oralidad*.

Oralidad

Es indiscutible que la primera forma en la que se comunicó el hombre fue por medio de sus expresiones kinestésicas y fonéticas, la utilización de un idioma que no es más que un código donde se establece una relación entre los fonemas y significados específicos para diferentes combinaciones de ellos de forma que al realizarse la comunicación entre individuos cualquiera que conozca las relaciones pueda decodificar esas combinaciones de fonemas, obtener y entender el mensaje original y transmitiendo así sus pensamientos o narrar hechos ocurridos.

Ese método de comunicación es muy volátil por sí solo (Romero, 2013), muchas tradiciones e historias lograron preservarse solo por medio de la oralidad, de manera natural los más viejos dentro de un grupo social contaban y enseñaban a los más jóvenes sus tradiciones y costumbres para que fueran contadas y ejecutadas de la misma forma que como se originaron, sin embargo esto presenta varios problemas:

-Está determinada por la capacidad de expresión del individuo, ejemplos claros como el tartamudeo o el miedo escénico puede crear ruido suficiente en la transmisión del mensaje para que no sea efectiva.

-La integridad de la información depende totalmente de la retentiva de los sujetos, ocasionando posibles cambios entre cada "versión" sin lograr llevar un registro de cuando se dio ese cambio.

-diferentes acentos y coloquialismos determinado por la costumbres de cada región puede llevar a confusiones y pérdida de algunas ideas o del contexto.

-la experiencia personal de cada individuo puede ser totalmente distinta y narrada influida por su sentir por lo que la información dada podría tener poca objetividad.

Por estas razones en la mayoría de las civilizaciones se apoyó en la escritura para lograr preservar la información con un soporte mediante el cual pudiera revivirse dicho registro, ya fuese en forma de cuentos, de leyendas, historia, entre otros. No significando esto que fue la única información existente en ese tiempo.

De la misma manera como considero debe existir un balance entre la oralidad y el uso de soportes escritos en el proceso que da respuesta a una necesidad informativa, debemos considerar el aporte informativo que representa un proceso de comunicación sin soporte.

> Admitir que un texto, en cualquier momento de su existencia fue oral, es tomar conciencia de un hecho histórico (…) se trata pues, de intentar ver la otra cara de este texto espejo, de hurgar en el azogue. Por encima de la evidencia de nuestro presente y de las racionalidades de nuestros métodos, queda un residuo: ese múltiplo sin origen unificador ni fin totalizador (…) y cuyo conocimiento pertenece al oído." (Zumthor c.p Massone, 2006, p44)

Otros aspectos claves de la oralidad que nos menciona Massone en su investigación de los estudios medievales de Paul Zumthor (Massone, 2006, p.44) son:

- La oralidad es un modo de pensamiento distinto al escrito pero no necesariamente opuesto.

- Hemos vivido en una sociedad compleja donde los textos son considerados garantía de orden.

- En la oralidad se ven involucrados elementos dinámicos y eventos que llegan a ser tan cotidianos que no atrae nuestra curiosidad.

- "su existencia es social, ya que implica un acto comunicativo de generación individual, que involucra tanto el hablar como el escuchar" (Massone, 2006, p44)

- "Los cambios sufridos por una comunidad tradicional (...) para hacer efectiva su comunicación remiten a la memoria colectiva" (Massone, 2006, p44)

Un punto donde se nota la importancia de la oralidad hoy día es en el aspecto legal, en muchos de los procesos legales se hace uso de testigos, testimonios, confesiones, opiniones profesionales y estos son registrados y analizados en base a las pruebas presentadas en texto legal que ya se tengan sobre un caso; La Ley Orgánica Procesal del Trabajo presenta lo siguiente en su artículo tres (3) "**Artículo 3.** El proceso será oral, breve y contradictorio, sólo se apreciarán las pruebas incorporadas al mismo conforme a las disposiciones de esta Ley, se admitirán las formas escritas previstas en ella." (Gaceta Oficial N° 37.504 de fecha 13 de agosto de 2002)

con esto podemos observar que se le da prioridad a la oralidad y se busca apoyo en los textos y no al contrario, en el caso del Código Orgánico Procesal Penal se da mayor prioridad a los textos y se busca gran apoyo en la oralidad.

> En consecuencia, las dos vertientes que hay actualmente es que lo oral tiende a lo social, mientras que lo escrito tiende a la formalización, al rigor de la doctrina, y entonces un derecho que se precie de tener su fundamento en una Carta Magna con fundamento social como la del 99, tiene que ser oral en general y, sobre todo, el derecho de los trabajadores. (Govea, 2006, p49).

Una razón por la que yo como investigador considero que todo proceso judicial en la actualidad se apoya o basa en la oralidad es para en cierta forma agilizar los procesos. En España los procesos jurídicos en el siglo XIII estaban caracterizados por algo denominado *solemnis ordo iudiciarius* (solemne orden judicial) donde las partes debían primero preparar su defensa o ataque, argumentos pero siempre por escrito, es descrito como un proceso lento, tedioso, complicado, formalista y riguroso; por otro lado el uso excesivo de la oralidad para los procesos judiciales hoy día con la cantidad de casos a ser atendidos empieza a retrasar los procesos, si un juez tiene muchos casos pendientes, debe designar una fecha a cada uno para las audiencias pertinentes para cada caso donde deben estar representadas todas las partes involucradas.

En la actualidad, la unión de la oralidad con los registros escritos van de la mano en muchas situaciones, ahora hay una tendencia a la oralidad multimedia que es la representación máxima de la unión de las dos vertientes, noticias, reuniones e incluso operaciones médicas se pueden realizar por medio de asistencia multimedia, a distancia y en tiempo real y por supuesto guardando el registro de lo ocurrido

4.2.- Los factores de preservación de la información digital.

4.2.1.- Estructura jurídico-legal de la información.

La protección Jurídica de la información se debería enfocar en el trato de la información como un ente creado por la capacidad cognitiva humana y toma diversas medidas para su protección como el registro por derechos de autor, patentes de invención, medio de expresión protegida constitucionalmente y consideraciones de formatos emergentes dentro de su propio género.

4.2.2.- Derecho de autor:

Para hablar de derecho de autor debemos primero entender la función de los derechos de autor y que es.

> Es el derecho que posee el autor sobre sus creaciones sean estas obras literarias, musicales, teatrales, artísticas, científicas o audiovisuales. Este derecho nace con el acto de creación y no por el registro de la obra, sin embargo es importante registrarlas para reforzar los derechos morales y patrimoniales del creador (SAPI, [s/f]a, p.1).

En derecho de autor en Venezuela tiene tres principios fundamentales:

1- El derecho de autor siempre recae en la persona natural que crea alguna obra producto del uso de su capacidad de raciocinio sin importar sus características de soporte, o intencionalidad y sin importar bajo quien quede registrado, en caso de que esos derechos correspondan a una persona jurídica ya sea por renuncia patrimonial del autor o algún convenio entre autor y la persona jurídica, serán considerados como los titulares de los mismos pero sólo en el aspecto patrimonial influyendo así en sus derechos de explotación.

2- El derecho de autor sólo protege la forma como se presenta una idea; el uso de la idea, su contenido técnico o ideológico no son objeto de protección en lo que se refiere a derecho de autor.

3- La duración de la protección que otorga la ley sobre derecho de autor en Venezuela según su artículo 25, dura mientras el autor se encuentre con vida y se extiende por 60 años que comienzan a contarse el primero de enero del año después de la muerte del autor (inclusive sobre las obras que no publicara en vida).

Bajo estos principios el Servicio autónomo de la propiedad intelectual (SAPI) define por separado los derechos de autor y los derechos patrimoniales

> <u>Derechos del autor:</u>
>
> Derechos Morales: Son los derechos inherentes al ser humano del autor de naturaleza inalienable, inembargable, imprescriptible e irrenunciable. Dichos derechos se encuentran enmarcados de la siguiente forma:

Derecho de Arrepentimiento y Modificación: Derecho del autor de retirar la obra del medio, o modificarla.

Derecho de Divulgación: Facultad del autor de decidir si publica su obra o no, y en qué forma lo hará.

Derecho de Paternidad: Derecho de exigir el reconocimiento como autor de la obra.

Derecho de Revelación o intimidad: El autor puede decidir divulgar una obra con su nombre, bajo un seudónimo, o de forma anónima. Esto no quiere decir que renuncie a la autoría de la obra.

Derecho de Integridad: Facultad de impedir cualquier deformación de la obra que pueda perjudicar el honor y reputación del autor. (SAPI, [s/f]a, p.1)

Derechos Patrimoniales:

Son los derechos que posee el autor o el titular del derecho el cual se caracteriza por ser transferible, temporal y renunciable.

Derecho de Reproducción: El autor puede obtener beneficio económico de las reproducciones o copias que se realicen de su obra.

Derecho de Distribución: Puesta a disposición del público del original o copias de la obra mediante su venta, alquiler, préstamo, o de cualquier otra forma.

Derecho de Comunicación Pública: La comunicación pública es todo un acto por el que una pluralidad de personas puede tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas.

Derecho de Transformación: Derecho del autor para autorizar y obtener una remuneración por las transformaciones que se hagan sobre la obra, como por ejemplo las traducciones.

En la Ley de derecho de autor, no son considerados objeto de Registro:

-Los textos de las leyes.

-Los juegos de cualquier naturaleza.

-Procedimientos matemáticos.

-Los manuales.

-Pensum de estudio.

-Decretos.

-Reglamentos oficiales.

-Tratados públicos.

-Decisiones Oficiales y demás Actos Oficiales. (SAPI, [s/f]a, p.1)

4.2.3.- Patentes de invención:

Las patentes se originan como reflejo de una innovación, su meta más importante a nivel industrial, es brindar protección a un activo intangible, "blindando" la idea a nivel legal dentro de aspectos económicos y corporativos. Según el Servicio autónomo de la propiedad intelectual (SAPI) entendemos por patente

> Es un derecho exclusivo que el Estado otorga al inventor, por un período de 5 a 10 años a partir del otorgamiento de la solicitud con el previo cumplimiento de los requisitos establecidos, con la cual se puede impedir que terceros, exploten su producto o procedimiento. Vencido el plazo de tiempo establecido esta pasa a dominio público. (SAPI, [s/f]b, p.1)

Las patentes otorgan la exclusividad únicamente para explotación comercial de un producto o uso de procedimientos, pero ¿en qué categorías podemos separar las patentes? Las modalidades de protección se muestran a continuación.

> Invención: El resultado del esfuerzo del ingenio humano que se concreta en un nuevo producto o procedimiento definido y que permiten en la práctica la solución de un problema técnico.
>
> Mejora: Toda nueva forma, reforma o modificación introducida en cosas ya conocidas que logre mayor economía, funcionalidad o perfección en los productos.
>
> Modelo Industrial: Se entiende por toda plástica combinada o no con colores, y todo objeto o utensilio industrial, comercial o doméstico que pueda servir de tipo para la producción o fabricación de otros y que se diferencien de sus similares por su forma o configuración distinta. (Ley de Propiedad Industrial, Artº. 22).
>
> Dibujo Industrial: Se entiende por toda disposición o unión de líneas, de colores y de líneas y colores destinadas a dar a un objeto industrial cualquiera una apariencia especial. (Ley de Propiedad Industrial, Artº. 22). (SAPI, [s/f]b, p.1)

4.2.4.- Protección legal:

El estado como primer garante de los derechos de sus ciudadanos posee una serie de artículos referidos a la protección de la información ya sea en temas de acceso, transparencia o confidencialidad; dentro de la constitución de la República Bolivariana de Venezuela podemos encontrar:

> Artículo 28: Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen

ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley.

Artículo 58: La comunicación es libre y plural, y comporta los deberes y responsabilidades que indique la ley. Toda persona tiene derecho a la información oportuna, veraz e imparcial, sin censura, de acuerdo con los principios de esta Constitución, así como a la réplica y rectificación cuando se vea afectada directamente por informaciones inexactas o agraviantes. Los niños, niñas y adolescentes tienen derecho a recibir información adecuada para su desarrollo integral.

Artículo 101: El Estado garantizará la emisión, recepción y circulación de la información cultural. Los medios de comunicación tienen el deber de coadyuvar a la difusión de los valores de la tradición popular y la obra de los o las artistas, escritores, escritoras, compositores, compositoras, cineastas, científicos, científicas y demás creadores y creadoras culturales del país. Los medios televisivos deberán incorporar subtítulos y traducción a la lengua de señas, para las personas con problemas auditivos. La ley establecerá los términos y modalidades de estas obligaciones.

Artículo 108: Los medios de comunicación social, públicos y privados, deben contribuir a la formación ciudadana. El Estado garantizará servicios públicos de radio, televisión y redes de bibliotecas y de informática, con el fin de permitir el acceso universal a la información. Los centros educativos deben incorporar el conocimiento y aplicación de las nuevas tecnologías, de sus innovaciones, según los requisitos que establezca la ley.

Artículo 223: La Asamblea o sus Comisiones podrán realizar las investigaciones que juzguen convenientes en las materias de su competencia, de conformidad con el Reglamento.

> Todos los funcionarios públicos o funcionarias públicas están obligados u obligadas, bajo las sanciones que establezcan las leyes, a comparecer ante dichas Comisiones y a suministrarles las informaciones y documentos que requieran para el cumplimiento de sus funciones.
>
> Esta obligación comprende también a los y las particulares; a quienes se les respetarán los derechos y garantías que esta Constitución reconoce.
>
> Artículo 337: El Presidente o Presidenta de la República, en Consejo de Ministros, podrá decretar los estados de excepción. Se califican expresamente como tales las circunstancias de orden social, económico, político, natural o ecológico, que afecten gravemente la seguridad de la Nación, de las instituciones y de los ciudadanos y ciudadanas, a cuyo respecto resultan insuficientes las facultades de las cuales se disponen para hacer frente a tales hechos. En tal caso, podrán ser restringidas temporalmente las garantías consagradas en esta Constitución, salvo las referidas a los derechos a la vida, prohibición de incomunicación o tortura, el derecho al debido proceso y los demás derechos humanos intangibles.

Aunado a la Constitución de la República Bolivariana de Venezuela y los artículos mencionados anteriormente que dan garantía de acceso, pluralidad y circulación de la información, contamos con el Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado. Publicado en la Gaceta Oficial N° 39.945 del 15 de junio de 2012 con el cual se fortalecen esos tres aspectos de protección de la información dados por la constitución y a su vez se incentiva la interoperabilidad de los entes gubernamentales. (Hernández, 2012)

4.2.5.- Nuevos formatos emergentes

Con el crecimiento exponencial de la tecnología se van creando nuevos tipos de medios y sistemas que quizás no consigan un lugar bien definido entre la tipología ya definida y explorada por los antiguos paradigmas de la bibliotecología. Así mismo existen activos intangibles como el software o bases de datos que en ocasiones no están definidos en una tipología dentro del derecho de autor o de patentes por el sistema legal venezolano.

> El software no calza cómodamente en las categorías legales tradicionales de las obras funcionales ni de las obras expresivas. El derecho autoral, luego el de patentes y ahora el de la [libertad de expresión] han sido forzados hasta tornarse irreconocibles con el fin de acomodar esta tecnología. Quizás la más razonable solución a esta dificultad sería la de colocar al software dentro de su propia categoría -no la de las patentes, el derecho de autor y ni siquiera la de la libre expresión-, una especialmente diseñada para coincidir con las características de este inusual híbrido legal. Desafortunadamente, probablemente sea demasiado tarde para devolver el reloj y tomar un camino tan razonable; así es que anticipamos que las instituciones jurídicas continuarán clasificando como 'funcional' o como 'expresivo' a una tecnología que podría ser ambas o ninguna. (Traducción de Christian Araya de Burk, Dan en "Copyrightable functions and patentable speech")

4.2.6.-Preservación digital:

Para conocer los factores de preservación de la información digital debemos primero ante todo entender que es preservación. "...la organización y programación de toda clase de actividades relacionadas con la conservación de las colecciones en general;..." (COMMA, 2001, p.59)

También debemos conocer todas las circunstancias bajo las cuales la información digital pueda sufrir un daño que la vuelva irrecuperable por lo cual podríamos considerarla perdida.

Dentro del entorno digital encontramos varios factores primordiales a proteger cuando se trata de pérdida de información: error de hardware, error humano (intencional o fortuito), error de software, software malicioso, incidencia del entorno (inundación, incendio, terremoto, explosión, derrumbes, contaminación, entre otros). RECOVERY LABS en uno de sus informes presenta los siguientes porcentajes en relación a esos factores basados en la frecuencia con la cual ese factor es el causante de pérdida de información.

Figura 2. Principales factores que causan una perdida de información, tomado de http://www.recoverylabs.com/wp-content/uploads/2014/03/ppales-factores-perdida-info-2003.jpg

Según un estudio de PricewaterhouseCoopers (PwC) una empresa mundial de asesoría gerencial en colaboración con Iron Mountain (profesionales en recuperación y preservación de información) destaca que el 46% de las empresas medias en Europa de forma errónea asumen que la responsabilidad de la protección de la información recae solo en el departamento de tecnología (PwC, 2014, p.4). Las repercusiones que puede tener la pérdida de información en una institución son incontables, gastos ocultos, retrasos en proyectos, daño a la reputación de la empresa, inoperatividad de algún departamento, daños colaterales a clientes, según el estudio sólo el 36% de las empresas cuenta con estrategias para contrarrestar el riesgo de pérdida y el 48% de las empresas dentro del estudio vio su reputación dañada por pérdida total o parcial de la información.

"Se podría decir que la mitad de los problemas que afectan a una computadora están relacionados con el software. La otra mitad es culpa de algún dispositivo de hardware dañado, mal configurado, incompatible, deficientemente refrigerado o que no cumple con los requerimientos mínimos para funcionar normalmente" (USERS, s/f, p18)

4.3.- Aspectos tecnológicos de la protección de la información digital

4.3.1.- Problemas de hardware

Respecto al hardware y sus posibles problemas los más destacados son:

Estabilidad**:** en informática se habla de que un componente es estable cuando tiene un nivel de fallo mínimo y cumple las funciones para la que fue diseñado a cabalidad de manera constante, algunos fallos comunes con respecto a la estabilidad son:

Pantalla azul: conocido en internet por sus siglas BSOD (Blue Screen Of Death) técnicamente es un error por el cual el sistema operativo Windows se ve forzado a detenerse se genera por diversos aspectos entre los que podemos incluir un módulo de memoria dañado, un error al leer un cluster del disco duro, fallo de los componentes de video entre muchos otros, cada error tiene un código hexadecimal que podemos usar para identificarlo e investigar el problema.

Reinicio espontáneo: en muchas ocasiones está relacionado al BSOD ya que al emitir el error la única opción que tiene el sistema es reiniciar, el segundo caso más común es debido a un sistema de protección del procesador al alcanzar una temperatura muy elevada que puede ser causado por fallas del cooler o un overclocking que hace trabajar más al procesador haciendo que aumente su temperatura de forma inusual o problemas con la fuente de poder, al no tener energía suficiente para mantener en funcionamiento el equipo.

Incompatibilidad**:** los problemas de incompatibilidad de hardware suelen ser difíciles de detectar ya que sus síntomas pueden ser aleatorios o inexistentes, muchos de los fabricantes poseen listas de compatibilidad de dispositivos y muchas piezas de hardware indican en sus empaques con que sistema operativo o en que la tarjeta madre (motherboard) tiene compatibilidad total, en caso de presentar incompatibilidad, los foros oficiales en línea del fabricante suelen tener tópicos respecto a este tema.

Requerimientos**:** tanto en hardware como en software existen tareas determinadas que posee un requerimiento mínimo para funcionar correctamente, en el caso de hardware un caso

muy común está relacionado a la fuente de poder, si el consumo de energía del hardware instalado en la tarjeta madre supera la capacidad de la fuente de poder que la surte puede traer como consecuencia que la computadora no enciende, que el dispositivo, la fuente de poder o la tarjeta madre se dañen por flujos irregulares de electricidad o que al activar el dispositivo se apague la computadora como protección.

Mal funcionamiento**:** todos los componentes de computadora son creados en masa y aun cuando en muchos casos su calidad sea alta siempre existe la posibilidad de que los componentes internos de alguna pieza de hardware estén flojos, con una soldadura deficiente o cualquier otro motivo por el cual el dispositivo no funcione correctamente, incluso si su instalación no se realiza de forma correcta, algún punto de contacto no esté en posición correcta podría provocar errores o desconexiones repentinas del dispositivo.

Falta de mantenimiento**:** muchos de los dispositivos de hardware como fuentes de poder, tarjetas de video, coolers, discos duros tienen componentes de funcionamiento mecánico, en su mayoría ventiladores para enfriar los dispositivos, si no se realizan mantenimientos regulares el polvo en el ambiente se acumula en rejillas o se mezcla con cualquier sustancia lubricante que posean los ventiladores creando una pasta que luego los inutiliza provocando un daño en el dispositivo.

Extinción del hardware**:** con el avance exponencial de la tecnología, cada año salen al mercado versiones nuevas y mejoradas de algunos dispositivos, incluso se ha acusado a varios desarrolladores de trabajar en base a una obsolescencia programada, al crear dispositivos con una vida útil corta calculada desde su diseño.

El que un hardware sea obsoleto, usualmente implica que su software asociado también pueda serlo, aumentando el chance de incompatibilidad y dificultando el acceso a la información que era mostrada a través de ella, para estos casos hay tres posibilidades para mantener el acceso.

1.- mantener el hardware original, realizando el mantenimiento pertinente

2.- encontrar algún hardware más actual que posea compatibilidad con hardware más antiguo

3.- emular el software usado en hardware antiguo mediante haciendo uso de un software especializado (incluso usado en algunos casos para emular otros sistemas operativos en entornos no compatibles)

4.3.2.- Errores de software:

En cuanto al software hay varios elementos que pueden causar pérdida parcial o total de la información, entre ellos podemos mencionar

Incompatibilidad por obsolescencia**:** El término obsolescencia se refiere a la antigüedad, vida útil en función del tiempo, así como pasa con el hardware también puede ocurrir con el software; Cuando las compañías de software crean versiones actuales con funciones nuevas, u otras compañías crean un software con funciones similares y logran dominar el mercado, los archivos de ese software antiguo en ocasiones no puede ser leído por el software actual o dominante, ocasionando esto una posible pérdida de información si no se mantiene el software anterior o si en las versiones actuales del mismo software no incluyen alguna compatibilidad con las versiones anteriores.

Un claro ejemplo de esto es la incompatibilidad que existía entre los documentos de Microsoft Office 97 y el Microsoft Office 2003, dado a que no se podía leer documentos de una versión creados en la otra. Asunto que la gente de Microsoft resolvió en su versión de Microsoft Office 2010 incluyendo en su opción “guardar como” un formato compatible de las versiones 97 y 2003.

Una manera sencilla (pero no infalible) de diferenciar compatibilidades de algunos archivos es por su extensión de archivo (siglas de término en el nombre de un archivo), algunos programas pueden mostrar un archivo de manera parcial, un ejemplo de ello es el Visor de imágenes de Windows que es capaz de abrir un archivo .GIF pero no muestra la animación correspondiente (de haberla)

Datos corruptos**:** distintos tipos de software funcionan con un conjunto de archivos propios para efectuar sus tareas y a su vez crean archivos adicionales donde se encuentra información específica que dan forma a un documento electrónico, si alguno de esos archivos sufre algún cambio en su contenido lógico, que falten datos o el sistema los considere no válidos puede desencadenar una falla de ese archivo.

Esto puede ocurrir debido a un virus informático, un mal funcionamiento del sistema operativo, a un cierre repentino del programa incluso en algunos casos errores de hardware que afecten al software (CD's rayados, sectores del disco duro dañados, entre otros).

Incompatibilidad por dualidad**:** La mayoría de los dispositivos que no son por definición *Plug & Play* requieren de controladores (drivers) y algunos sistemas operativos poseen controladores estándar para ciertos dispositivos como tarjetas de red, tarjetas de red inalámbricas, tarjetas de video, entre otras.

En algunos casos al instalar los controladores creados por la compañía a la que pertenece dicho dispositivo queda en ejecución junto a los controladores estándar del sistema operativo y puede crear conflictos al seguir ordenes de ambos controladores al tiempo por lo que se presenta una malfunción del dispositivo de manera aleatoria que puede ocasionar pérdida de información sobre la acción ejecutada por el dispositivo, causando archivos corruptos, daño del hardware o disparidad en la comparación de datos con un servidor.

Disparidad comparada: En la actualidad se hace uso recurrente de la llamada Nube, que no es más que un servidor dedicado en paridad con un dispositivo o usuario para almacenar todo aquello que se le indique (usualmente elementos multimedia); Esto presenta una gran ventaja a la hora de proteger información respecto al riesgo que representa un dispositivo móvil como soporte.

En cualquier sistema o software que se hace uso de un servidor remoto conectado a internet, además de los riesgos comunes a los que se exponen en su forma física, siempre existe otro riesgo, la conexión. Si al comparar los datos del servidor con el cliente en tiempo real, no coinciden, se intenta interrumpir o se produce un error podría perderse los datos al momento de la transferencia de datos

Debilidades de seguridad: El software es creado por humanos y como tal puede tener defectos, defectos que van más allá de algo relacionado con su entorno de programación, reacción del software ante fallas de hardware, su periodo de creación; La seguridad que ofrece el software se puede ver vulnerada si al momento de la programación no se consideraron ciertas debilidades que pueden ser explotadas por terceros para obtener acceso a datos de un computador sin tener los permisos necesarios, la Common Weakness Enumeration posee una lista con los 25 más peligrosos errores de software para el 2011, creada como una investigación conjunta del instituto SANS, el MITRE y otras compañías dedicadas a la seguridad de software en Europa y Estados Unidos.

Esta lista posee aspectos altamente técnicos, donde para cada debilidad, su ranking en la lista general se provee en el cuadro entre corchetes, el CWE ID en su página provee un link donde se da una explicación de la debilidad nombrada, métodos para detectarlos, detalles técnicos y consejos para su prevención. Cada tabla a su vez nos presenta una categorización de la lista en tres aspectos principales.

La lista de CWE con las 25 debilidades y errores de software más importantes es la siguiente.

Tabla 1.Lista de errores y debilidades de software tomada de http://cwe.mitre.org/top25/index.html

Rank	Score	ID	Name
[1]	93.8	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[2]	83.3	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[3]	79.0	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
[4]	77.7	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[5]	76.9	CWE-306	Missing Authentication for Critical Function
[6]	76.8	CWE-862	Missing Authorization
[7]	75.0	CWE-798	Use of Hard-coded Credentials
[8]	75.0	CWE-311	Missing Encryption of Sensitive Data
[9]	74.0	CWE-434	Unrestricted Upload of File with Dangerous Type
[10]	73.8	CWE-807	Reliance on Untrusted Inputs in a Security Decision
[11]	73.1	CWE-250	Execution with Unnecessary Privileges
[12]	70.1	CWE-352	Cross-Site Request Forgery (CSRF)
[13]	69.3	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[14]	68.5	CWE-494	Download of Code Without Integrity Check
[15]	67.8	CWE-863	Incorrect Authorization
[16]	66.0	CWE-829	Inclusion of Functionality from Untrusted Control Sphere
[17]	65.5	CWE-732	Incorrect Permission Assignment for Critical Resource
[18]	64.6	CWE-676	Use of Potentially Dangerous Function
[19]	64.1	CWE-327	Use of a Broken or Risky Cryptographic Algorithm
[20]	62.4	CWE-131	Incorrect Calculation of Buffer Size
[21]	61.5	CWE-307	Improper Restriction of Excessive Authentication Attempts
[22]	61.1	CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
[23]	61.0	CWE-134	Uncontrolled Format String
[24]	60.3	CWE-190	Integer Overflow or Wraparound
[25]	59.9	CWE-759	Use of a One-Way Hash without a Salt

Para hacerse una idea más concreta, tenemos una lista separada por categorías de errores que podemos ver a continuación.

Interacción insegura entre componentes: Estas debilidades están relacionadas a las formas inseguras en a que la data es enviada y recibida entre componentes, módulos, programas, procesos, hilos o sistemas separados. (Traducción propia).[6]

Tabla 2.Lista de errores por interacción insegura de componentes tomada de http://cwe.mitre.org/top25/index.html

Rango en la lista	Detalle
[1]	Neutralización impropia de elementos especiales usados en un comando SQL
[2]	Neutralización impropia de elementos especiales usados en un comando del SO
[4]	Neutralización impropia de entrada durante generación de la página web
[9]	Carga no restringida de un archivo con una extensión de archivo peligrosa
[12]	Falsificación de solicitud cruzada
[22]	Redirección de la URL a una página de no confianza

Gestión de recursos riesgosos: Las debilidades en esta categoría están relacionadas a las formas en las que el software no maneja de manera apropiada la creación, uso, transferencia o destrucción de importantes recursos del sistema. (Traducción propia).[7]

[6] These weaknesses are related to insecure ways in which data is sent and received between separate components, modules, programs, processes, threads, or systems. tomado de http://cwe.mitre.org/top25/index.html

[7] The weaknesses in this category are related to ways in which software does not properly manage the creation, usage, transfer, or destruction of important system resources. tomado de http://cwe.mitre.org/top25/index.html

Tabla 3. Lista de errores por gestión de recursos riesgosos tomada de http://cwe.mitre.org/top25/index.html

Rango en la lista	**Detalle**
[3]	El buffer copia sin chequear tamaño de la entrada.
[13]	Limitación impropia de una dirección dentro de un directorio restringido.
[14]	Descarga del código sin chequeo de integridad.
[16]	Inclusión de funcionalidad desde una esfera de control no es de confianza.
[18]	Uso de una función potencialmente peligrosa.
[20]	Cálculo incorrecto de tamaño del buffer
[23]	Cadena de formato no controlada
[24]	Desbordamiento de enteros

Defensas porosas: Las debilidades en esta categoría están relacionadas a técnicas defensivas que usualmente son usadas incorrectamente, abusadas o simplemente ignoradas. Traducción propia[8]

Tabla 4.Lista de errores consideradas defensas porosas tomada de http://cwe.mitre.org/top25/index.html

Rango en la lista	**Detalle**
[5]	Autenticación desaparecida para función critica.
[6]	Autorización desaparecida.
[7]	Uso de credenciales incluidas en el código del programa.
[8]	Perdida del encriptado en datos sensibles.
[10]	Dependencia de entradas no confiables en decisiones de seguridad.
[11]	Ejecución con privilegios innecesarios.
[15]	Autorización incorrecta.
[17]	Asignación de permisos incorrectos para un recurso crítico.

[8] The weaknesses in this category are related to defensive techniques that are often misused, abused, or just plain ignored. tomado de http://cwe.mitre.org/top25/index.html

[19]	Uso de un algoritmo de encriptado roto (defectuoso) o peligroso.
[21]	Restricción impropia de exceso de intentos de autenticación.
[25]	Uso de un algoritmo Hash de un solo sentido sin usar bits aleatorios

4.3.3.- Errores humanos:

La relación del factor humano en la pérdida de información puede desencadenar la eliminación, robo, sustitución, modificación o siembra de información, el hecho de que estas acciones sean deliberadas o no, se determina después de una investigación. En la mayoría de los casos la intencionalidad de esas acciones no producen un gran cambio en el resultado y las prevenciones a tomar son de utilidad en cualquiera de los dos casos.

Dentro de las causas más comunes podemos encontrar:

Mal manejo de hardware o software: el desconocimiento en el funcionamiento o manejo de algún dispositivo o software puede causar pérdida de información, en la mayoría de los dispositivos el software está diseñado específicamente para ese hardware, en ocasiones los botones del software no son tan intuitivos como podría creer el programador, unido a la posibilidad de que las instrucciones dadas pueden ser muy generales o no incluya instrucciones sobre una posible incompatibilidad (con el sistema operativo o con otro software que se ejecuta al mismo tiempo).

Aquí podemos incluir situaciones tan simples como presionar el botón de “guardar” en vez del botón “guardar como..” perdiendo la versión anterior del mismo trabajo, presionar el botón de “cargar” en vez de “guardar”, desactivar alguna opción de autoguardado y cerrar el programa sin guardar la información del documento confiando en que estaba activa, acostumbrarse a un estándar de combinación de teclas para acciones concretas y accionar de manera automatizada puede resultar en un error humano por ejemplo: redactando un documento presionar la combinación de teclas “control + x” para cortar ese segmento, si por error se selecciona otro fragmento y se presiona la combinación de teclas “control + c” que es para copiar el documento cuando se consideraba pegar el fragmento cortado (considerando que en un teclado la letra “V” está justo a la derecha de la “C”), el primer fragmento se sobrescribe en el portapapeles y se pierde.

Incluso no seguir las instrucciones del programa; en ocasiones algunos software realizan tareas de carga y modificación de registros y da la instrucción al usuario de esperar y no cerrar

el programa, el no seguir esta instrucción puede ocasionar errores de registros en el programa o en el sistema pudiendo inutilizar el software o crear archivos corruptos irrecuperables.

Mal manejo de datos: muchas compañías a nivel mundial poseen servidores con datos privados muy sensibles como su dirección completa, números telefónicos privados, información médica, pólizas, los datos de la tarjeta de crédito de un cliente, o datos de su cuenta bancaria. Los servidores y servicios de atención al cliente tienen acceso parcial o total a estos datos desde su sistema, si por alguna circunstancia revela datos o rompe algún protocolo de seguridad de la empresa o de seguridad informática dentro de la compañía estos datos están en riesgo de pérdida.

Instalación de actualizaciones o controladores no oficiales: si bien es cierto que en algunos casos programadores expertos crean sus propios controladores para dispositivos liberando algunas acciones del hardware o mejorando la efectividad de un software, el instalar actualizaciones o controladores no oficial puede conllevar a una falla del sistema, crear una incompatibilidad desconocida o forzar a una pieza de hardware a trabajar por sobre su capacidad segura o puede contener algún código adicional que busque acceder a datos importantes en nuestro computador lo que sin duda nos puede llevar a pérdida de información

Vandalismo informático: acciones con fines contrarios al resguardo y protección de la información: robo, sabotaje, acceso no autorizado

> "la manipulación fraudulenta de las computadoras con ánimo de lucro, la destrucción de programas o datos, el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad" (Gildardo, s/f, p58)

4.3.4.- Software malicioso

El software malicioso también conocido como malware es un software diseñado y creado para destruir, modificar, sustraer datos o para crear accesos eludiendo la seguridad del computador para usos posteriores, algunos necesitan la interacción directa del usuario para ejecutarse y su acción puede ser prevenida por una revisión antes de su ejecución por parte de

un antivirus y siguiendo un comportamiento cauteloso a la hora de abrir archivos de procedencia dudosa, si recibe un correo sospechoso o localiza algún archivo ejecutable del cual no conozca su procedencia es mejor no abrir el archivo.

Otros tipos de malware proceden de algunos programas gratuitos que contienen un código oculto, al permitir la instalación de estos programas gratuitos se le concede acceso a nuestro sistema sin saberlo, algunos de estos programas son los conocidos P2P (peer to peer) o redes de punto a punto que nos permiten compartir programas, imágenes, o cualquier elemento multimedia con otros usuarios sin conocer su ubicación exacta dando acceso a puertos de comunicación en nuestro computador; hoy día es una de las formas más comunes en las que las personas dan acceso a otros sin saber por el alto consumo de programas piratas o contenido multimedia no autorizado para distribución por esta vía.

Pueden hacerse pasar por archivos del sistema o mimetizarse entre archivos de uso común como videos, imágenes, archivos de audio, documentos entre otros, en esos casos la información del documento se corrompe y usualmente queda en un estado irrecuperable.

En los inicios de la computación los virus o gusanos tenían tareas solo de destrucción de datos, inhabilitación de dispositivos o incluso para realizar bromas, con la importancia creciente de la información en la economía, y el boom en el alcance de la tecnología muchos de los virus tienen como objetivo sustraer información importante del computador donde se encuentre, usar cuentas de correo ajenas para enviar correos basura, promover publicidad no deseada, cambiar alguna configuración del sistema para usar un determinado software, obtener claves de acceso, entre otros.

4.3.5.- Incidencias del entorno:

Aclarando en primera instancia que no me referiré a este punto como desastres naturales como suele ser tratado en toda la bibliografía consultada dado a que una inundación por falla de una tubería, algún incendio, una explosión o daños por contaminación son incidencias de sistemas creados por el hombre en la mayoría de sus casos y deben ser

considerados como factores que ponen en riesgo al entorno que resguarda en forma analógica la información tanto o más que una incidencia de índole totalmente natural como un terremoto.

Como se mencionó anteriormente incluso en el mundo digital debemos mantener medidas para la protección de lo analógico; bien podemos subir una foto a la nube pero esa nube es un servidor que posee de igual forma un ente físico, si ese ente físico sufre daños o es vulnerado de alguna forma esos datos sufrirán el mismo destino de su servidor.

Los daños al hardware pueden provenir de incidencias bruscas repentinas como un incendio, un terremoto o una inundación, la contaminación, la humedad, la temperatura, fallos eléctricos, golpes a las piezas del hardware por caídas o por razones intencionales, campos electromagnéticos fuertes, incluso de insectos y roedores

4.4.- Los métodos más eficientes de protección de la información digital

Luego de analizar los factores más importantes para los planes de preservación de la información digital debemos identificar formas eficientes para proteger la información tomando en consideración los factores anteriores.

4.4.1.- La nube (cloud computing):

"La nube es un sistema computacional inteligente, complejo y poderoso en el cielo, al cual la gente simplemente se conecta" (Hamm, 2008, citado en Rueda, 2010, p73)

La nube (o cloud computing) son servidores físicos conectados a internet de manera constante con espacios reservados asociados a cuentas o usuarios específicos con un entorno de interacción totalmente digital, muy accesibles y compatibles con gran número de dispositivos mientras posean conexión a la red. Presentan una ventaja absoluta en el tema de distribución y acceso de información. Existen nubes públicas y nubes privadas con público y propósitos distintos según sus necesidades.

El sistema de nube se puede separar en tres capas: Software como servicio, Plataforma como servicio e Infraestructura como servicio, más conocidos en inglés por sus siglas Saas, Paas e Iaas respectivamente

Software como servicio (Saas): Es la capa más alta, ofrece una solución rápida y completa basada en software en la cual el usuario no necesita ocuparse de nada relacionado a los aspectos vitales para el sustento del sistema, la compañía que ofrece el servicio es la encargada de su total funcionalidad y de garantizar el servicio, algunos ejemplos a mencionar son los servidores de correo electrónico y entornos para compartir elementos multimedia, Gmail, Hotmail, Youtube, Dailymotion, Grooveshark entre otros.

Plataforma como servicio (Paas): Es la capa media, ofrece los recursos de infraestructura, sistema operativo, middleware, es decir toda la plataforma necesaria para desarrollo, almacenamiento y uso de aplicaciones y datos propios del cliente y a su vez la posibilidad de compartirlos, un ejemplo de esto es Google app engine que trabaja con diversos lenguajes de programación (javascript, ruby, phyton) y posee características básicas de forma gratuita.

Infraestructura como servicio (Iaas): Es la capa inferior, ofrece los recursos de infraestructura solamente, también conocido como Hardware as a service (Haas), se ofrecen las capacidades de conectividad y procesamiento de datos. El cliente puede solicitar ancho de banda, la capacidad de almacenamiento, memoria, firewalls y servidores dedicados según sus necesidades, usualmente los servicios de Iaas son usados por compañías grandes, algunas compañías que ofrecen este servicio son Bluelock, Gogrid y Amazon web services.

Otras de las grandes ventajas que ofrece la nube son:

-Rápida incorporación de la información a la plataforma.

-Disponible al público en medida casi instantánea.

-Menor requerimiento de espacio físico.

-Reduce costos en almacenamiento.

-Migración de datos más rápida.

-Ahorro en licencias de software.

La seguridad en la nube es difícil de generalizar dado que cada compañía dueña del respectivo servidor toma medidas de seguridad diferentes, lo más común es el uso de contraseñas, imágenes de verificación, transmisión de datos codificados, códigos de verificación, chequeo de localización de acceso.

Debemos recordar que ningún sistema de protección de información es 100% infalible y el uso de la nube tiene también algunas desventajas:

-Si donde nos encontramos no disponemos conexión a la red no podremos acceder a ninguna información.

-Los servidores que conforman la nube poseen de igual forma un ente analógico, si en el datacenter donde se encuentra nuestra información sucede algo que comprometa el funcionamiento de los servidores o su seguridad física, nuestra información está en riesgo de inaccesibilidad parcial o en el peor de los casos pérdida total.

-Dado a que en los servidores de la nube se concentra mucha información, suelen ser blanco de piratas informáticos, y si la compañía dueña de los servidores no aborda de manera efectiva la seguridad de su red puede comprometer información delicada de sus clientes.

-Las compañías que ofrecen estos servicios si no llevan un control de los contenidos permitidos pueden ser acusados de infringir leyes y cerrados ocasionando pérdidas masivas de información, tal es el caso de Megaupload, una compañía que ofrecía servicio de hosting, usado masivamente para guardar contenido que subían sus usuarios que en forma mayoritaria infringía los derecho de autor de casas disqueras, canales de televisión o productoras de cine.

El FBI intervino y cerró las operaciones de Megaupload, aun cuando había información que si infringía los derechos de autor, existía un alto índice de información personal y legal que se perdió, incluso se llegó a hablar de que algunos usuarios estaban planeando demandar al FBI por la pérdida de esa información legal.

4.4.2.- Discos duros:

Las diferencias entre los disco duros convencionales de disco magnético y los disco duros sólidos conocidos también como SSD (solid state drive) que usa tecnología de chip son bastante notables, los disco duros SSD aun cuando son más nuevos tienen ventajas y desventajas respecto a los magnéticos y viceversa, veamos las ventajas y desventajas de cada uno.

Disco duro magnético: También conocidos por sus siglas HDD, consisten en un disco magnetizado y posee una aguja magnética para leer la información, en su evolución los puertos de conexión más conocidos son los SCSI (popular para servidores), los IDE y los SATA para los internos y USB para los externos; miden su velocidad en revoluciones por minuto (RPM), su memoria caché es medida en megabytes y su capacidad de almacenamiento es medida en Gigabytes la mayoría o en Terabytes para los de última generación.

Tabla 5.Tabla comparativa de ventajas y desventajas del disco duro magnético (elaboración propia)

VENTAJAS	DESVENTAJAS
Mucha capacidad de almacenamiento a bajísimo costo en comparación con otras formas de almacenamiento (CDs, DVDs, BLU-RAY pen drives)	En condiciones no controladas como calor, humedad, golpes son muy vulnerables a la pérdida de datos
Rápido acceso a los datos con respecto a discos ópticos (CDs, DVDs, BLU-RAY, etc)	Consume más electricidad que otros tipos de almacenamiento, debido a la necesidad de mantener el disco magnético girando a miles de RPM
En condiciones normales el funcionamiento de un disco duro es prolongado, puede durar muchos años.	
Alto índice de recuperabilidad de información después de un desperfecto del dispositivo	

Disco rígido: muy nombrados como SSD, el término “rígido” es debido a que no usa componentes mecánicos para su funcionamiento, su funcionamiento en estructura es básicamente igual al de las memorias USB dado que trabajan con tecnología de chip. Su puerto de conexión es SATA por lo cual es compatible con computadoras no tan actuales (de 3 a 5 años atrás), su velocidad de lectura es medido en megabytes por segundo (MB/s), en muchos SSD la memoria caché es de 256 kilobytes y su capacidad de almacenamiento es considerablemente menor a su contraparte magnética.

Son unidades de almacenamiento con una velocidad de lectura mucho mayor a la de un disco duro magnético, sin el riesgo de pérdida de información por golpes o mal funcionamiento mecánico, son más ligeros, delgados y su consumo de energía es notablemente menor a un disco duro convencional lo que los volvió una opción atractiva para nuevos dispositivos móviles como tablets y laptops

Tabla 6.Tabla comparativa de ventajas y desventajas del disco rígido (elaboración propia)

VENTAJAS	DESVENTAJAS
más ligeros, delgados y consumen menos energía, lo que los HDD, haciéndolos la opción perfecta para dispositivos portátiles	Son de alto costo y de menor capacidad de almacenamiento que un HDD convencional.
Mejoras constantes en la tecnología SSD, pudiendo mejorar su capacidad, velocidad y otras debilidades en algunos años	la vida útil es más corta, el tipo de memoria que utiliza tiene una cantidad de escrituras en memoria limitado
Los SSD más rápidos alcanzan velocidades de hasta 500 MB/s	no existe un estándar de velocidad para los SSD
Físicamente más duraderos	Son más vulnerables a fallas eléctricas
Compatible con los conectores SATA	La recuperación de datos en un SSD es más difícil y en algunos casos imposible

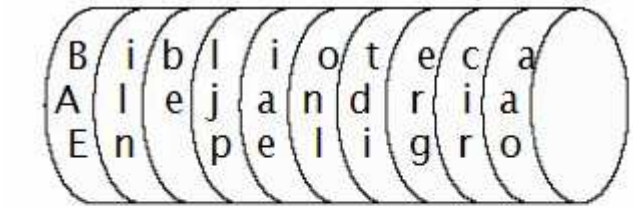
4.4.3.- Encriptado:

Conocido también como cifrado dado a que encriptado es una palabra no reconocida por la R.A.E es definido por SECOMDATA como: “La encriptación es el proceso para volver ilegible información considerada importante. La información una vez encriptada sólo puede leerse aplicándole una clave.” (SECOMDATA, 2009, p.1)

Ese proceso tiene como finalidad el proveer una mayor seguridad a la información, restringiendo el acceso a información confidencial en el entorno donde se encuentra almacenado o en el proceso de transmisión de datos, para que en caso de ser copiados o interceptados no pueda recuperarse la información sin la clave correcta para revertir el proceso de cifrado.

Breve historia del cifrado:

La escitala: sistema de encriptado usado (aproximadamente) en el siglo V antes de Cristo, esta forma de encriptado consiste en recubrir un rodillo llamado escitala con una tira de cuero de forma diagonal y escribir el mensaje sobre el cuero de manera regular, al retirar la cinta de cuero solo se podían apreciar letras sin ningún sentido, la clave para descifrar el mensaje era posee una escitala de la longitud y grosor exactos para lograr leer el mensaje original, (Martínez, 2011) a continuación un ejemplo.



Cualquiera que consiga la tira solo veria esto:
BAE-iln-be -ljp-iae-onl-tdi-erg-cir-aao
Cuando el mensaje original es:
Biblioteca Alejandria en peligro

Figura 3. Representación gráfica de una escitala con mensaje encriptado (elaboración propia)

Cifrador de Polybios: Es un sistema de encriptado por sustitución usado en el siglo II antes de Cristo, que consiste en una tabla de coordenadas con una combinación única para cada letra, el mensaje era escrito en coordenadas de la tabla, a continuación un ejemplo

Tabla 7.Ejemplo de tabla de codificación del cifrador de polybios (elaboración propia)

	A	**B**	**C**	**D**	**E**
A	*a*	*b*	*c*	*d*	*e*
B	*f*	*g*	*h*	*i/j*	*k*
C	*l*	*m*	*n*	*o*	*p*
D	*q*	*r*	*s*	*t*	*u*
E	*v*	*w*	*x*	*y*	*z*

Al leer este mensaje

AEDCACDEAECAAA ADAE ABBDABCABDCDDDAEACCDCACDBBBDAA y proceder al intercambio donde cada par de letras representan una coordenada en la tabla podemos obtener lo siguiente “Escuela de Bibliotecología”

Cifrado de César: Usado en el siglo I antes de Cristo, trabaja también con a base de sustitución simple, en este caso sustitución monoalfabética (letra por letra) al tener el mensaje original, su criptograma consistía en intercambiar cada letra del mensaje original por la tercera siguiente en el alfabeto, en el caso de su adaptación al castellano, la “A” se sustituye por la “D”, la “B” por la “E”, a continuación un ejemplo.

Tabla de sustitución:

Parte superior: letra del mensaje original

Parte inferior: letra a sustituir para encriptar

Tabla 8.Tabla codificadora del sistema de cifrado de César (elaboración propia)

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Mensaje original: Escuela de Bibliotecología.

Mensaje encriptado: Hvfxhod gh Eleolrwhfrorjld.

Disco de Alberti: creado cerca del año 1466 Leon Battista Alberti creó un sistema polialfabético de encriptación que posee dos anillos con letras, el externo (fijo) contiene un alfabeto (donde faltaba las letras H,J,K,U, W y la Y) en el sentido de las agujas del reloj y agrega los números del 1 al 4 siguiendo después de la "Z" con un total de 24 caracteres, que es usado para determinar las letras del mensaje original y en su anillo interno (móvil) contiene un alfabeto en un orden distinto, dada la movilidad del anillo interior de este disco, hay una posibilidad de usar 24 alfabetos distintos, en muchos casos cada cierta cantidad de palabras (o letras) cambiaban el abecedario a usar girando la rueda, (Martínez, 2011) a continuación un ejemplo.

Figura 4.Representación gráfica disco de Alberti tomado de https://www.trifariam.com/estilos/imagenes/alberti.png

Mensaje original: Biblioteca

Mensaje encriptado girando la rueda cada 2 letras: kvgvr&okb

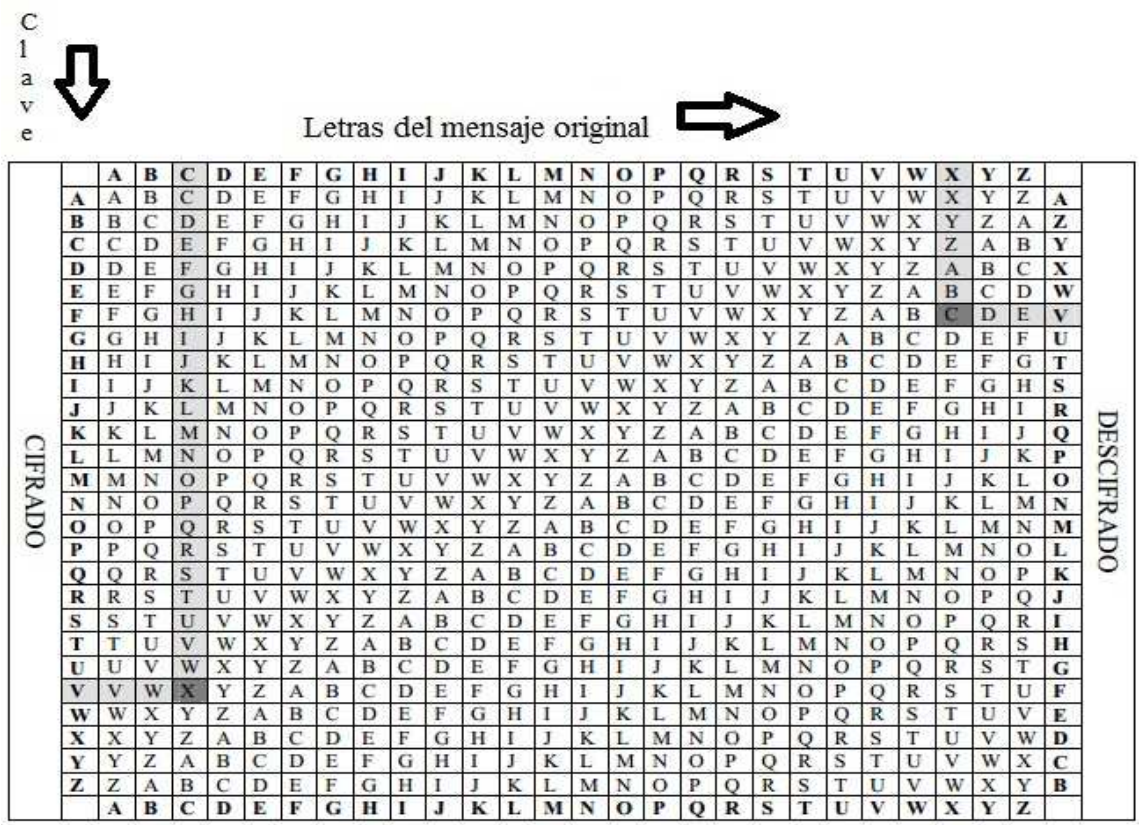
(Otros sistemas polialfabéticos son: La rueda de Jefferson, y el disco de Wheatstone)

Máquina Enigma: Con el diseño original de Arthur Scherbius, en 1923 Scherbius se asoció a Willie Korn, dueño de la compañía Enigma Chiffiermaschinen (de la cual toma el nombre) y vendían al público una versión con tres rotores polialfabéticos que intercambiaban las letras bajo una clave para proteger secretos comerciales, en 1926 la compañía pasó a manos del gobierno alemán y su versión comercial fue retirada del mercado, comenzó a ser usada por la Marina en Alemania durante la II Guerra Mundial, quienes modificaron la máquina para incorporar un cuarto rotor y aumentar su seguridad.

La máquina Enigma dio pie a otras máquinas de cifrado como las desarrolladas por el criptólogo sueco Boris Hagelin aproximadamente por el año de 1930, basadas en el sistema de cifrado Beaufort y la desarrollada por Frederick FriedMan cerca de 1940 que también funcionaba con rotores de sustitución polialfabética.

Criptosistema de Vigenére: un sistema polialfabético que usa dos elementos principales, una clave repetida constantemente y una tabla, la tabla está diseñada con el Algoritmo de César (usar la siguiente letra del abecedario), a continuación un ejemplo.

Tabla 9.Tabla explicativa de uso del criptosistema de Vigenére (elaboración propia)



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	**A**
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	**Z**
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	**Y**
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	**X**
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	**W**
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	**V**
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	**U**
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	**T**
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	**S**
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	**R**
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	**Q**
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	**P**
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	**O**
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	**N**
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	**M**
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	**L**
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	**K**
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	**J**
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	**I**
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	**H**
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	**G**
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	**F**
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	**E**
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	**D**
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	**C**
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	**B**
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	

Mensaje original: Quiero más libros

Clave: EBA

Tabla 10.Tabla ejemplo del criptosistema de Vigenére (elaboración propia)

Mensaje	q	u	i	e	r	o	m	a	s	l	i	b	r	o	s
Clave	E	B	A	E	B	A	E	B	A	E	B	A	E	B	A
Resultado	u	v	i	i	s	o	q	b	s	p	j	b	v	p	s

Cifrados matemáticos:

En la actualidad los métodos de encriptado ya no son solo por sustitución simple o polialfabéticos, para dar un rango mayor de posibles combinaciones y volver el cifrado más seguro, se usan fórmulas matemáticas. Algunos de los cifrados matemáticos más conocidos son.

1.-Cifrado RSA: Las siglas de este sistema son las iniciales de los apellidos de sus creadores: Ron **R**ivest, Adi **S**hamir y Len **A**dleman es uno de los cifrados modernos que hace uso de fórmulas matemáticas para cifrar y descifrar los mensajes.

El mensaje se cifra asignando a cada letra un entero. Estos enteros se agrupan en bloques que forman enteros más grandes.

Para encriptar usando el cifrado RSA se usa la función:

$\mathbf{C} = \mathbf{M}^{\mathbf{e}} \mod \mathbf{n}$ (módulo n referido a la aritmética modular)

donde:

M = mensaje original

C= mensaje cifrado

n = p × q con p y q enteros primos grandes (normalmente de 200 dígitos)

e = número primo con (p -1)(q -1)

2.-Criptografía elíptica: Sistema de encriptado propuesto por Neal Koblitz de la Universidad de Washington y Victor Miller de IBM en 1985 usando un grupo de puntos racionales en una curva elíptica. Este método ofrece una fortaleza similar al sistema RSA mediante el uso de una clave de menor tamaño, lo que optimiza la velocidad y consumo de energía en un computador.

Hasta la fecha era uno de los sistemas de encriptado con mayor fortaleza debido a la dificultad del problema del logaritmo discreto de las curvas elípticas

3.-Criptografía cuántica: Es un método basado en el principio de incertidumbre de Heisenberg que dicta que es imposible medir cualquier par de variables físicas por ejemplo la posición y cantidad de movimiento de un objeto sin alterar su valor real, mientras se intente una medición más precisa, más se altera su valor original.

Suponiendo un sistema de comunicación básico formado por un emisor y un receptor donde ninguno posee una clave para encriptar el mensaje y los posibles valores para crearla radica en 4 bits diferentes: representados en grados son: 0°, 45°, 90° y 135°, podemos decir que hay dos valores rectos y dos valores diagonales, asignaremos un valor de bit a cada uno

Tabla 11.Tabla de asignación de valores a la representación en grados para su equivalencia en bit (elaboración propia)

Grados	0°	45°	90°	135°
Representación	**--**	\	|	/
Valor bit	1	1	0	0

El emisor creará una clave usando para ello estos valores, emitiendo una ristra de bits (bit string) aleatoria y agregando una base existiendo dos bases posibles: rectilínea (+) o diagonal

(X), la base rectilínea sólo admitirá valores rectilíneos, el filtro diagonal puede admitir valores diagonales y el 50% de las veces un valor rectilíneo de forma aleatoria.

Tabla 12.Tabla explicativa de valores aceptados por cada tipo de ristra de bits (bitstring) (elaboración propia)

Base	**Admite**
X	**/ (0) , \ (1) , -- (1) , | (0)**
+	**-- (1) y | (0)**

El emisor crea una ristra de bits aleatorios que sólo él conoce y debe aplicar una base aleatoria para cada valor, el receptor como no conoce todavía la base que uso el emisor, aleatoriamente asigna una base a cada valor, al terminar la recepción de datos, el emisor y el receptor deben comparar sus bases y solo las que coincidan son tomadas en cuenta para formar la clave encriptada.

Tabla 13.Tabla explicativa del funcionamiento del proceso de encriptado cuántico (elaboración propia)

Bits aleatorios del emisor	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**1**
Base aleatoria del emisor	+	+	X	+	X	X	X	+
Representación en grados enviada por el emisor	|	--	\	|	\	/	/	--
Base aleatoria del receptor	+	X	X	X	+	X	+	+
Representación en grados recibida	|	/	\	/	--	/	--	--
COMPARACIÓN DE BASES								
Clave secreta final	0		1			0		1

Con la ristra de bits 01101001, luego de comparar las bases del emisor y receptor solo coincidieron 4 de las representaciones dadas, formando la clave 0101.

4.4.4.- Respaldos de información:

Cuando una información es única el riesgo de pérdida al que se expone es muy alto, Uno de los métodos más eficientes para evitar la pérdida total de la información es su reproducción constante; podemos dar sus ejemplos más destacados como la Biblia, el Corán y muchos otros textos religiosos que mantienen su contenido intacto después de más de mil años.

Lo que hizo posible que hoy día podamos leer pasajes exactos luego de todo ese tiempo, fue la reproducción de la misma información de forma constante, con el dominante paradigma físico el crear miles de copias de un ejemplar suponía sólo una función de acceso de información más que de su protección. Después de la creación de sistemas como la imprenta, y herramientas analógicas electrónicas como disquetes, unidades ZIP, CD, entre otras; la reproductividad por protección o respaldos empezaron a ser mucho más comunes.

Los respaldos tienen dos objetivos primordiales:

- Proteger la información contenida en un archivo individual o en una colección de su pérdida total.

- Permitir la restauración de un archivo a un estado funcional, en caso de su pérdida previa.

Aun cuando las circunstancias sean únicas y en algunos casos exista una pérdida de información parcial el uso de respaldos es una de las recomendaciones más comunes. Debemos considerar que no sólo los archivos que contengan escritos específicos, tablas de cálculo, fotografías o archivos de audio son los únicos respaldos importantes; el software también sufre cambios importantes con actualizaciones o configuraciones que en caso de pérdida no son sencillos de restaurar y deben ser considerados como material a respaldar.

Tiempos de respaldo: Los archivos al igual que la información puede cambiar en el transcurso del tiempo, al ser los gerentes o custodios de una información, debemos conocer de antemano la frecuencia con la que estos archivos son modificados y en base a ello, planificar la estrategia de tiempo y tipo de respaldo.

Respaldo completo: Como su nombre indica consiste en crear un respaldo completo de toda la información de la que se dispone, es un proceso que consume más recursos, memoria y más tiempo al momento de su ejecución pero menos tiempo a la larga para el usuario.

Garantiza una copia exacta del 100% de la información de la que se dispone; se recomienda un respaldo completo si la información no varía en un tiempo prolongado.

Respaldo diferencial: En este tipo de respaldos se toma una fecha de referencia y todos los respaldos subsecuentes se realizará para todos los archivos nuevos o creados desde esa fecha hasta la actualidad, aumentando el tamaño del respaldo y el consumo de memoria y tiempo de ejecución a medida que transcurre el tiempo, ejemplo:

Si se toma como fecha de referencia el lunes y se pretende hacer un respaldo diferencial diario, el martes se respaldan todos los datos del día lunes y el martes; al hacer un respaldo el miércoles, se tomarán los archivos del lunes, del martes y del miércoles (aumentando cada vez más el tamaño del respaldo).

Se recomiendan respaldos diferenciales si la información varía en un periodo medio.

Respaldo incremental: Posee una similitud con el respaldo diferencial respecto a que ambos tipos de respaldo, solo respaldan archivos con información nueva ya sea creada o modificada; en los respaldos incrementales la fecha a consideración para el respaldo es la fecha del último respaldo, ya sea completo o incremental, tiene el menor consumo de recursos en la red y el menor tiempo de ejecución posible, pero el mayor tiempo a la larga para el usuario, un ejemplo:

Si el último respaldo completo fue el día lunes, y hacemos un respaldo incremental diario, el martes se respaldan todos los archivos nuevos o modificados del día lunes después del respaldo completo y del mismo martes hasta que se ejecute el respaldo; el miércoles sólo se respaldan los archivos del martes después del respaldo y los creados el miércoles y así sucesivamente.

Se recomiendan respaldos incrementales sólo si la información varía en períodos cortos.

Movilidad de la información digital: En los inicios de la computación, la movilidad de la información a gran escala dependía del desmantelamiento y traslado de algunos equipos; lo que suponía gastos enormes en recursos como personal, tiempo y dinero. Esa carga fue luego aliviada por elementos móviles compatibles con los computadores donde se alojaba la información, ya el hardware de los computadores no debía ser trasladado para llevar la información de un lugar a otro y dado a que era más económico generarlos unido a su cualidad de ser generados en masa y a la facilidad de duplicar la información que contenían, estos medios de almacenamiento se tornaron muy famosos y versátiles, dentro de los más conocidos en una breve compilación encontramos:

Tarjetas perforadas: con su origen en 1801 a manos de Joseph Marie Jacquard las primeras tarjetas perforadas contenían información de los diseños a tejer en el telar según las perforaciones en las tarjetas y la secuencia de ellas; en 1887 Herman Hollerith patenta las tarjetas perforadas y reduce a menos de la mitad el tiempo que tomaba procesar los censos en Estados Unidos el censo de 1880 fue concluido en 1888 y el censo de 1890 se procesó para el año de 1893, ese evento se considera el primer procesamiento de datos de forma automatizada. En 1911 Hollerith fundó la Tabulating Machine Company que años después junto a unas fusiones con otras compañías en 1924 pasó a llamarse International Business Machines (IBM).

Cintas magnéticas: son un soporte de almacenamiento que consiste en una cinta plástica recubierta con material magnético como óxido de hierro, en estos dispositivos se puede almacenar video, audio y datos de forma secuencial, para lograr acceder a un bloque de la cinta donde se encuentra la información debe accederse primero al bloque anterior (para acceder a N debe acceder primero a N-1).

Existen muchos dispositivos asociados a las cintas magnéticas, como el magnetófono, betamax, VHS, discos flexibles (floppy), entre otros, con la capacidad de grabar, borrar y leer la información por medio de una bobina electromagnética. Esta cinta se encuentra enrollada en dos carretes dentro de una cubierta de plástico rígido para evitar el contacto con el exterior y así proteger su información. Logrando resguardar grandes cantidades de información en unos casetes altamente portátiles, ya que el cartucho y los disquetes son de tamaño pequeño.

Discos compactos: En el año de 1980 aproximadamente la compañía *Philips* desarrolló un sistema óptico digital con principios similares a los de la cinta magnética, con el uso de discos de policarbonato de plástico, recubrimientos de aluminio (inicialmente) sellados con laca y la unidad lectora con láser, al igual que las cintas magnéticas evolucionó dentro de su misma metodología para ofrecer mayor capacidad de almacenamiento y la capacidad de escribir en los discos desde equipos caseros con un láser de baja potencia, en orden cronológico podemos mencionar: los disco compacto de sólo lectura (CD-ROM), disco compacto de escritura (CD-R), disco compacto re escribible (CD-RW) los discos versátiles digitales (DVD) y discos blu-ray (BRD)

Memorias bus de serie universal (USB): estas memorias se incorporaron al mercado cerca del año 2000 gracias a la colaboración entre *IBM* y *Trek Technology* como una solución portátil de almacenamiento dada la poca capacidad de almacenamiento de los discos de cinta magnética y la incapacidad de escribir datos a nivel personal en las primeras generaciones de discos compactos; sus primeras unidades flash o pen-drive (llamadas así por su tamaño y portabilidad) tenían capacidad de 16 megabytes de almacenamiento, en la actualidad existen memorias USB con almacenamiento mayor a 64 gigabytes con velocidades de lectura y escritura mayor.

Memorias secure digital (SD): estas memorias fueron creadas por Panasonic, son utilizadas en dispositivos altamente portátiles tales como cámaras digitales, teléfonos móviles, computadoras portátiles y consolas de videojuegos, su avance es rápido y sus diseños han pasado de dimensiones de 32x24 milímetros (SD) a 21,5x20 milímetros (miniSD) y 11x15 milímetros (microSD), junto a esto se han creado diferentes adaptadores que permiten una compatibilidad de puertos mucho mayor, de microSD a USB, de microSD a miniSD y de miniSD a SD haciéndolas líderes actuales en tipo de almacenamiento portátil.

Antivirus: Un antivirus es cualquier programa o sistema que: prevenga la activación de los virus, su propagación dentro de un sistema y que los elimine y provea herramientas para la reconstrucción de archivos o de áreas afectadas por los virus informáticos.

Los software antivirus trabajan basándose en vacunas o firmas, que son segmentos de códigos maliciosos que comparan con el archivo que están chequeando, y en caso de estar infectados con el código malicioso pueden intentar eliminar solamente el código malicioso que contiene, eliminar el archivo por completo, o colocar el archivo en cuarentena moviéndolo a un lugar dentro del computador donde se restringe su ejecución esperando una posible solución quizás en una actualización del antivirus.

Dentro de los antivirus podemos encontrar tres tipos principales:

Antivirus heurísticos: El archivo a verificar, desensambla el código del programa a verificar y analiza qué haría el programa de ser ejecutado, si el antivirus encuentra acciones en el código del programa que son propias de un virus y no muy usuales en un programa, da el aviso de alerta. El único problema con estos antivirus son los llamados *falsos positivos*, en ocasiones programas destinados a modificar redes o algunos drivers de tarjetas de red, enrutadores o software de redes virtuales al trabajar con los puertos de conexiones puede indicar la presencia de un virus cuando no es cierta.

Antispyware: Los spyware son virus que tienen el objetivo de recopilar datos del sistema y personales, para enviarlos a terceros, normalmente compañías de publicidad, algunos datos que pueden buscar son cuentas de correo electrónico y el password, dirección IP y DNS, teléfono, país, páginas que busca el usuario una lista de las páginas que visita, básicamente ver qué temas le interesan (basado en palabras claves de los buscadores), el tiempo que el usuario esta en ellas y la frecuencia con la que regresa, crea una lista del software que tiene el usuario y en casos más graves datos mucho más importantes como números de tarjeta de crédito y cuentas bancarias.

Antispam: El spam son mensajes no deseados, usualmente mensajes de correo electrónico, el software antispam tiene una lista negra de direcciones IP de las cuales bloquea inmediatamente cualquier correo enviado desde esa dirección, también se usan filtros con palabras clave y patrones de mensajes similares que el usuario reciba de manera constante, todavía no existe un anti spam que sea 100% efectivo, en ocasiones podemos encontrar correos en la lista de spam que no son malintencionados ni con intenciones comerciales, por lo cual debemos de igual forma hacer un chequeo manual de los correos

Emulación**:** Primero debemos entender que emular en su concepto más simple nos habla de imitación, o compararse con algo, pero en la informática es básicamente cuando un entorno o arquitectura busca funcionar como otra, un emulador puede imitar las funciones de otro dispositivo de hardware o un sistema operativo, los dos emuladores más comunes son los emuladores de consolas de videojuegos, la máquina virtual.

Emuladores de consolas: mediante uso de los recursos del computador, su función es crear las condiciones necesarias para ejecutar el software diseñado para una consola en específico o placas que representan una plataforma distinta al computador, dispositivos de hardware con características muy específicas con la sola función usar juegos de video; usualmente se utilizan emuladores de consolas descontinuadas para mantener el acceso a los juegos únicos.

Máquina virtual: es un software con el que se puede simular un computador en el cual podemos instalar programas, simular hardware que no se encuentra en el computador en ese momento e incluso hacer uso de otros sistemas operativos en la máquina sin correr el riesgo de dañar registros del sistema operativo que tengamos como principal, es usual para usuarios de un sistema operativo probar otro con una máquina virtual para probar el desempeño de algunas aplicaciones de forma momentánea (instalar Windows en una Mac, o Linux en Windows). Dentro de los emuladores de sistemas operativos podemos mencionar: *Bluestacks* que emula el sistema operativo Android, *Cygwin* emula Linux en Windows y *Parallels* que puede emular Windows o Linux en una computadora Mac

Muchas de las compañías que pertenecen al modelo de Infraestructura como servicio (Iaas) en la nube hacen uso de máquinas virtuales para darle al cliente un entorno según sus necesidades sin necesariamente hacer cambios fuertes en hardware, o software en sus servidores.

CAPÍTULO V - LINEAMIENTOS PARA LA PROTECCIÓN DE LA INFORMACIÓN DIGITAL

Lineamientos de protección de la información digital

Los lineamientos aquí escritos tienen como finalidad asegurar que la información digital permanezca inalterable, utilizable, legible, de fácil acceso autorizado y resguardada adecuadamente en caso contrario. Estos lineamientos son pasos y consideraciones a tomar para lograr el objetivo planteado.

Para ello comencé por considerar las fortalezas de la legislación venezolana, para luego entrar en el núcleo del mundo digital actual con seguimientos a tomar en cuenta con el uso de la nube, dado que los computadores en su composición cuentan con hardware y software se dan recomendaciones para evitar los problemas relacionados a estos puntos planteados en el capítulo IV de esta investigación, de igual forma como el computador tiene su mayor interacción con el humano se consideraron normas para evitar los errores humanos más comunes al interactuar con sistemas de información digital.

Como todo ese conjunto de partes que representa a la información digital tiene un ente analógico que normalmente se encuentra en uso ininterrumpido, deben tomarse las previsiones necesarias para ser protegido de las incidencias del entorno, por lo cual lo consideré otro punto esencial para la elaboración de estos lineamientos.

Finalmente en las consideraciones adicionales se dan recomendaciones que no solo están relacionadas con la protección de la información digital sino que también afectan su efectividad de uso, movimiento y velocidad de recuperación.

A continuación se presenta el esquema de los lineamientos.

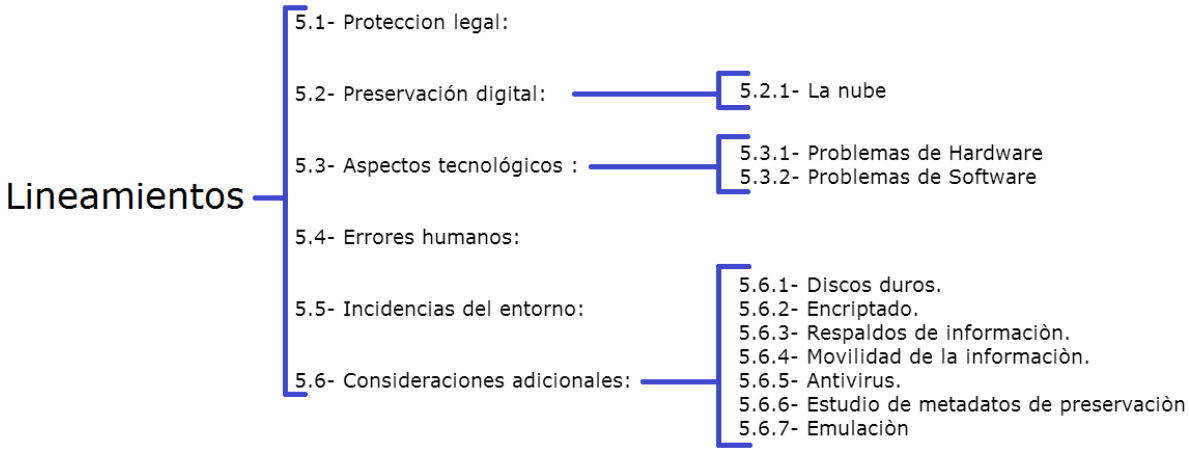


Figura 5.Esquema de los lineamientos propuestos como resultado de la investigación (elaboración propia)

5.1.- Protección legal:

Hacer cumplir los artículos 28, 58 y 101 de la Constitución citados anteriormente en el punto 4.2.4- del mismo nombre para garantizar la protección en materia de acceso a la información, en aspectos como la pluralidad, privacidad y formas de difusión para todo tipo de usuario, y en casos donde se presenten situaciones no estipuladas de manera intuitiva en una categoría o que presente algún vacío legal (como los nuevos formatos emergentes con elementos quizás no considerados todavía en las leyes) contactar a entes expertos en ese tipo de material y realizar los estudios necesarios para determinar las acciones a tomar para garantizar los derechos de los usuarios y la protección de la información.

De igual forma hacer respetar las leyes concernientes a las patentes de invención y al derecho de autor en los aspectos morales y patrimoniales estipuladas por el SAPI (Servicio autónomo de la propiedad intelectual) así como sus excepciones. En el caso de los formatos emergentes hacer los estudios o tomar las decisiones pertinentes para mantener el estado de derecho según sea requerido; existen activos intangibles como el software o bases de datos que en ocasiones no están definidos en una tipología dentro del derecho de autor o de patentes por el sistema legal venezolano.

5.2.- Preservación digital:

Con la interconectividad actual entre computadores y el compartir de la información casi sin limitaciones de distancia, tiempo y cantidad (en cuanto a las capacidades digitales claro está) el uso de la nube como punto central de la información digital actual amerita ser objeto de estudio y de esta forma entender sus partes para saber las acciones y prevenciones a tomar según sea el caso.

5.2.1- La nube:

Recordando que la nube son servidores físicos conectados a internet de forma constante y puede ser separado en tres capas: Software como servicio, Plataforma como servicio e Infraestructura como servicio, debemos tomar en cuenta distintos tipos de prevenciones para cada capa

Software como servicio (Saas):

En esta capa la responsabilidad del resguardo físico de los servidores y la programación que protege a los servidores de ataques externos está completamente de parte del prestador de servicios, en estos casos nuestra responsabilidad está en proteger nuestros datos sensibles que permiten acceso a los servidores del prestador de servicios (usuarios, contraseñas, imágenes de verificación, etc) las medidas a nuestro cargo son simples pero importantes.

- *De ser posible no anotar el usuario y clave en lugares de fácil acceso para terceras personas como: hojas sueltas, archivos desprotegidos*
- *No aceptar ayuda de terceras personas que no sean de su confianza para manipulación de su cuenta.*
- *Guardar los datos en sistemas protegidos como correos electrónicos o usar opciones de encriptado en los archivos donde se encuentre la información sensible.*
- *Evitar usuarios y claves repetitivas en diferentes cuentas/sistemas.*
- *Seguir los consejos de seguridad brindados por el prestador de servicios.*
- *No Ingresar datos sensibles en computadores de uso público.*
- *De ser necesario el uso de un computador público, use el modo privado del explorador (browser) en uso para evitar que la información sensible se guarde en el cache.*
- *Estar consciente de las distintas técnicas de scam y phishing para robo de información, así como el uso de la ingeniería social.*

Plataforma como servicio (Paas):

En esta capa se deben seguir los procedimientos anteriores al iniciar sesión en la página que ofrece dicho servicio, sin embargo, cualquier aplicación creada en la plataforma ofrecida por ellos debe contar con aspectos de seguridad a nivel de programación (cosa que ya no es responsabilidad de la empresa prestadora del servicio).

- *Ver las certificaciones y protocolos de seguridad que ofrece un servicio de PAAS antes de usar sus servicios.*
- *Ver el desempeño de la compañía prestadora del servicio en auditorías externas (SSAE 16 tipo II o su versión internacional ISAE 3402 tipo II).*
- *No descartar el uso de plataformas basadas en software libre mientras confirme buenos niveles de seguridad y que posean alta compatibilidad con otras plataformas para posible migración de datos, ej Cloud Foundry (basado en lenguaje Ruby), OpenShift (basado en Linux Red Hat), Apache Stratos (trabaja con Php)*

Infraestructura como servicio (Iaas):

En la infraestructura como servicio ya que es básicamente un espacio en blanco donde se elabora una plataforma y un software propio, debemos estar conscientes que gran parte de la responsabilidad de la seguridad de los datos está a cargo de la persona o empresa que contrata el servicio, por lo que debemos considerar ciertas interrogantes como:

- *¿Qué datos que requiere la plataforma para su funcionamiento?*
- *¿Qué tipo de datos sensibles va a manejar la plataforma que se desarrolla en ese servicio?*
- *¿Qué tipo de seguridad física y lógica ofrece el proveedor?*
- *¿Hemos definidos los parámetros de seguridad para distintos tipos de datos?*
- *¿Está sujeta la data resguardada a propiedad intelectual?*
- *¿Ofrecerá servicios relacionados a transacciones?*
- *¿El servicio cumple con los estándares internacionales de cifrado?*
- *¿Cómo es el proceso de eliminación de datos al migrar a otro servicio similar?*

5.3.- Aspectos tecnológicos de la protección de la información digital

"Se podría decir que la mitad de los problemas que afectan a una computadora están relacionados con el software. La otra mitad es culpa de algún dispositivo de hardware dañado, mal configurado, incompatible, deficientemente refrigerado o que no cumple con los requerimientos mínimos para funcionar normalmente" (USERS, s/f, p18)

5.3.1.- Problemas de Hardware

Los problemas más destacados del hardware son aquellos que comprometen la estabilidad del sistema. La mayoría de los problemas de estabilidad en hardware recaen en componentes con poco mantenimiento, hardware instalado de forma errónea o incompatibilidad de componentes (por diseño o por obsolescencia) las principales medidas que podemos tomar son:

Incompatibilidad**:**

- *Al instalar nuevas piezas de hardware ver sus requerimientos e incompatibilidades probadas.*
- *Al instalar los controladores de un hardware, solo hacer uso del software certificado por el fabricante.*

Mal funcionamiento:

- *Verificar que los componentes de hardware a instalar tengan todos sus puntos de contacto en posición correcta en el puerto/slot correcto.*
- *Verificar que los cables unidos al dispositivo de hardware se encuentren en buen estado.*
- *En caso de que el sistema arroje mensajes de error o se detenga de manera abrupta, leer el mensaje y tomar las medidas necesarias.*
- *Verificar condiciones o entes externos que puedan generar una irregularidad en el funcionamiento del hardware.*

Requerimientos:

- *Verificar semanalmente en las páginas de los fabricantes del hardware sí disponen de una actualización de los controladores que puedan resolver algún problema existente.*

Extinción del hardware:

- *Verificar semestralmente las listas de compatibilidad del hardware no elemental para el funcionamiento del computador (scanners, tablas de dibujo, impresoras, routers).*
- *Si el hardware en uso no posee un dispositivo más actual que pueda sustituirlo, considerar el uso de emuladores y migración de formatos.*

Falta de mantenimiento:

- Realizar limpieza regular de los componentes de hardware, sobre todo aquellos que posean componentes de funcionamiento mecánico (ventiladores, botones, engranajes)

Con el avance exponencial de la tecnología, cada año salen al mercado versiones nuevas y mejoradas de algunos dispositivos, incluso se ha acusado a varios desarrolladores de trabajar en base a una obsolescencia programada, al crear dispositivos con una vida útil corta calculada desde su diseño.

El que un hardware sea obsoleto, usualmente implica que su software asociado también pueda serlo, aumentando el chance de incompatibilidad y dificultando el acceso a la información que era mostrada a través de ella, para estos casos hay tres posibilidades para mantener el acceso.

1.- mantener el hardware original, realizando el mantenimiento pertinente

2.- encontrar algún hardware más actual que posea compatibilidad con hardware más antiguo

3.- emular el software usado en hardware antiguo mediante haciendo uso de un software especializado (incluso usado en algunos casos para emular otros sistemas operativos en entornos no compatibles)

5.3.2.- Errores de software:

Para evitar la pérdida de información a causa de errores de software, de acuerdo a estos lineamientos se sugieren unas medidas para contrarrestarlas siguientes fallas:

Incompatibilidad por obsolescencia:

- *Al hacer uso de un programa, verificar que se encuentre actualizado.*
- *En caso de no usar la última versión de un programa, verificar que los archivos que ejecuta son compatibles con la versión con la que se dispone.*
- *En caso de que los archivos en resguardo no sean compatibles con las versiones nuevas del programa(s) hacer un estudio de necesidad de migración de datos.*
- *Al hacer una migración de los archivos a una versión nueva, comprobar la integridad de los archivos (que no cambie el formato de la información, que no pierda calidad o que no se encuentre incompleto).*
- *En caso de ser un programa comercial, llevar seguimiento de las actualizaciones y saber si la empresa sigue ofreciendo soporte para el programa o versión en uso.*

Datos corruptos:

- *Instalar programas originales.*
- *No instalar cracks o actualizaciones creadas por terceros.*
- *Seguir las instrucciones del programa para guardar o cargar información (en caso de que la tenga).*
- *Garantizar el suministro eléctrico durante la manipulación de archivos mediante un UPS (UninterruptedPowerSupply) o en su defecto generadores de electricidad.*
- *Comprobar el estado del hardware antes de realizar transmisión de datos entre dispositivos (puertos en buen estado, cables conectados correctamente).*
- *Limpiar el sistema operativo de posibles virus con capacidad de modificar archivos.*

Incompatibilidad por dualidad:

- *Instalar solo controladores certificados por la compañía diseñadora del hardware*
- *Verificar la compatibilidad de los controladores con el sistema operativo en uso*
- *Verificar que el sistema operativo no se encuentra usando un controlador propio de forma paralela.*

En algunos casos al instalar los controladores creados por la compañía a la que pertenece dicho dispositivo queda en ejecución junto a los controladores estándar del sistema operativo y puede crear conflictos al seguir ordenes de ambos controladores al tiempo por lo que se presenta una malfunción del dispositivo de manera aleatoria que puede ocasionar pérdida de información sobre la acción ejecutada por el dispositivo, causando archivos corruptos, daño del hardware o disparidad en la comparación de datos con un servidor.

Disparidad comparada:

- *Verificar que se tenga una conexión a internet o en su defecto a la intranet que almacene los datos.*
- *Verificar la conexión sea estable.*
- *De ser posible crear un soporte local de la información que se va a subir a la nube.*
- *Verificar la seguridad de la conexión a los servidores.*

Debilidades de seguridad:

- *Usar antivirus de calidad, con certificados actualizados.*
- *Chequear semanalmente si existen actualizaciones para el antivirus en uso*
- *Realizar dos escaneos semanales de forma regular.*
- *Si se sospecha de una violación de seguridad, física o desde un servidor externo, hacer un escaneo de antivirus al momento.*
- *Revisar las actualizaciones del sistema operativo que puedan resolver problemas de seguridad.*
- *Cambiar las claves cada 120 días, en caso de una violación de seguridad hacer el cambio de claves inmediatamente.*

5.4.- Errores humanos:

Los sistemas tienen la necesidad de interactuar en mayor o menor medida con el factor humano, por ende parte de la responsabilidad más allá de lo administrativo también recae en las personas (la eliminación, robo, sustitución, modificación o siembra de información), para evitar dichos problemas hacemos las siguientes sugerencias para

5.4.1.-Mal manejo de hardware o software:

- *Evaluar al personal en el manejo de los recursos digitales que disponga la UI.*
- *Ofrecer cursos o contratar especialistas para contrarrestar las debilidades que pueda tener el personal.*
- *Explicar al personal las distintas razones que pueden generar perdida de información en los dispositivos de hardware*
- *Explicar al personal las distintas razones que pueden generar perdida de información en los programas que usa la UI.*

5.4.2.-Mal manejo de datos:

- *Crear una clasificación de niveles acceso a la información que posee la UI según la legalidad de su divulgación.*
- *Crear un protocolo de seguridad para el manejo de cada tipo de información según su clasificación.*
- *Designar un personal con función de analista para que clasifique la información de la que dispone la UI en los diferentes niveles de acceso.*

5.4.3.-Instalación de actualizaciones o controladores incorrectos o no oficiales:

- *Al instalar un controlador para un hardware nuevo, si este no está incluido buscarlos en la página oficial del producto.*
- *No instalar controladores creados por terceras personas que ofrecen un desempeño mayor en los dispositivos.*
- *Si bien es cierto que en algunos casos programadores expertos crean sus propios controladores para dispositivos liberando algunas acciones del hardware o mejorando la efectividad de un software, el instalar actualizaciones o controladores no oficial puede conllevar a una falla del sistema, crear una incompatibilidad desconocida o forzar a una pieza de hardware a trabajar por sobre su capacidad segura o puede contener algún código adicional que busque acceder a datos importantes en nuestro computador lo que sin duda nos puede llevar a pérdida de información*

5.4.4.-Vandalismo informático:

- *Evitar el acceso al servidor físico de personal no autorizado.*

- *De poseer conexión a internet, hacer chequeos semanales con un programa antivirus.*
- *Si la conexión pasa por un router o switch, configurar un firewall para evitar accesos no autorizados.*
- *Si el sistema operativo posee un firewall propio, no desactivarlo (salvo que cree conflicto con el firewall del router).*
- *acciones con fines contrarios al resguardo y protección de la información: robo, sabotaje, acceso no autorizado*

5.4.5.-Software malicioso:

- *Evitar el ingreso a páginas que ofrecen software gratuito o ilegal.*
- *No instalar programas que comprometan la seguridad de la información en el computador.*
- *Aprovechar las herramientas de uso e intercambio de archivos en la nube sin necesidad de descarga.*
- *en términos de conexión o El software malicioso también conocido como malware es un software diseñado y creado para destruir, modificar, sustraer datos o para crear accesos eludiendo la seguridad del computador para usos posteriores, algunos necesitan la interacción directa del usuario para ejecutarse y su acción puede ser prevenida por una revisión antes de su ejecución por parte de un antivirus y siguiendo un comportamiento cauteloso a la hora de abrir archivos de procedencia dudosa, si recibe un correo sospechoso o localiza algún archivo ejecutable del cual no conozca su procedencia es mejor no abrir el archivo.*

Otros tipos de malware proceden de algunos programas gratuitos que contienen un código oculto, al permitir la instalación de estos programas gratuitos se le concede acceso a nuestro sistema sin saberlo, algunos de estos programas son los conocidos P2P (peer to peer) o redes de punto a punto que nos permiten compartir programas, imágenes, o cualquier elemento multimedia con otros usuarios sin conocer su ubicación exacta dando acceso a puertos de comunicación en nuestro computador; hoy día es una de las formas más comunes en las que las personas dan acceso a otros sin saber por el alto consumo de programas piratas o contenido multimedia no autorizado para distribución por esta vía.

Pueden hacerse pasar por archivos del sistema o mimetizarse entre archivos de uso común como videos, imágenes, archivos de audio, documentos entre otros, en esos casos la información del documento se corrompe y usualmente queda en un estado irrecuperable.

En los inicios de la computación los virus o gusanos tenían tareas solo de destrucción de datos, inhabilitación de dispositivos o incluso para realizar bromas, con la importancia creciente de la información en la economía, y el boom en el alcance de la tecnología muchos de los virus tienen como objetivo sustraer información importante del computador donde se encuentre, usar cuentas de correo ajenas para enviar correos basura, promover publicidad no deseada, cambiar alguna configuración del sistema para usar un determinado software, obtener claves de acceso, entre otros.

5.5.- Incidencias del entorno:

Debemos recordar que incluso la nube que muchos ven como la opción definitiva contra la perdida de información no son más que muchos servidores conectados entre sí, que poseen de igual forma un ente analógico que es igual de vulnerable a la incidencia del entorno como cualquier otro tipo de soporte con la ventaja de que su capacidad de almacenamiento es exponencialmente mayor a cualquier soporte no electrónico o digital y con capacidad multimedia, de esta forma hay cuidados que son muy importantes para proteger la información contra la incidencia del entorno, entre las cuales sugerimos.

- *Ubicar los servidores ó computadores en bases o muebles que los mantengan por encima del nivel del suelo.*
- *Juntar y organizar los cables que puedan necesitar los computadores de forma organizada.*
- *Ubicar los servidores ó computadores lejos de ventanas y aspersores contra incendios.*
- *En caso de no ser posible ubicarlos fuera del alcance de los aspersores, los equipos electrónicos deben estar protegidos por algún mueble que deje correr el agua sin que entre en contacto con los equipos.*
- *Verificar el estado de las instalaciones eléctricas.*
- *Solo conectar los servidores ó computadores en reguladores eléctricos o U.P.S (Uninterrupted Power Supply).*
- *Mantener los servidores a temperaturas entre 20 y 25 grados centígrados.*

- *Mantener la humedad entre 40 y 55% en donde se encuentren los servidores ó computadores.*
- *Limpiar mensualmente los componentes internos del computador, evitando la acumulación de polvo en ventiladores y rejillas de respiradero para que fluya el aire con normalidad para evitar así un aumento de temperatura fuera del uso normal de los componentes.*
- *No usar aspiradoras para limpiar componentes eléctricos debido a que crean acumulación de energía estática que puede dañar los componentes de hardware de forma irreparable.*
- *Ubicar los servidores en un área de uso único para ello.*
- *Verificar la existencia de insectos y roedores en el edificio donde se encuentran ubicados los servidores.*
- *Al notar deterioro en el cableado de los servidores a causa de insectos o roedores, realizar una fumigación y cambiar el cableado inmediatamente.*

5.6.- Consideraciones adicionales.

5.6.1.- Discos Duros:

Dado a que no todas las variables en la protección de la información digital son iguales (hardware, software, recurso humano, medio ambiente, etc) hay sugerencias que podrían ser mejores o peores dependiendo de la realidad a la que está sometida, por ello se harán una serie de sugerencias para ciertas situaciones:

En un entorno de oficina regular donde los computadores donde se encuentren resguardados los datos no necesite una alta movilidad, donde el entorno pueda ser controlado en mayor medida se recomienda el uso de discos duros magnéticos:

- *Ofrecen mayor capacidad de almacenamiento a menor costo.*
- *La velocidad de acceso es más rápida que un disco óptico.*
- *En un entorno controlado su durabilidad es altamente prolongada.*
- *En caso de fallas del dispositivo la probabilidad de recuperación de datos es mayor.*

En un entorno donde la necesidad de movilidad de la información en uso y captura multimedia de datos se recomienda el uso de discos duros rígidos:

- *Usan tecnología chip.*
- *La tecnología SSD está en continuo desarrollo por lo que podemos esperar mejor rendimiento, mayor espacio y otras ventajas en unos años.*
- *la velocidad de lectura es notablemente mayor.*
- *El consumo de energía es bastante reducido.*
- *No presenta daños por componentes mecánicos.*
- *Compatible con los tipos de conectores más nuevos en el mercado.*
- *Está considerado como nuevo estándar para equipos portátiles de alto rendimiento.*

5.6.2.- Encriptado:

Sea cual sea el sistema, el uso o el tipo de datos que se resguardan de forma digital se recomienda siempre contar con un sistema de encriptación (codificación).

El estándar más probado y reconocido es el AES desarrollado por dos criptologos belgas, con variables de 128, 192 y 256 bits, es hasta ahora el único sistema aprobado por la NSA para codificar información clasificada.

Sobreentendiendo que básicamente ningún sistema de encriptado es 100% impenetrable, el dar una dificultad mayor al acceso no autorizado ayuda significativamente con la protección de la información desde el punto de vista de acceso, no solo evitándolo al momento sino creando registros que nos permitan identificar una amenaza y reforzar el sistema según las características del invento de violación de seguridad.

5.6.3.- Respaldos de información:

El crear un respaldo de la información, ya sea análoga o digital es un proceso natural de su ciclo sin embargo, de no tener un plan o un criterio de que respaldar, como y cuando respaldarlo el factor de perdida de la información sería cuestión de suerte por ello debemos determinar cada cuanto deberíamos respaldar la información sabiendo que cada tipo de archivo tiene un manejo distinto.

5.6.3.1.- Tiempos y tipos de respaldo

Dado a la gran cantidad de cambios que puede tener un material digital, y sus distintas funcionalidades por tipología la UI debe tener distintos planes en los tiempos de respaldo según su necesidad basada en la creación de nuevo material, las recomendaciones siguientes están enfocadas en mantener un balance entre la protección de la información contra la pérdida total y el mayor aprovechamiento de los recursos (humano/tecnológico) de la UI. (A los efectos de estas recomendaciones, debe considerarse las modificaciones de archivos ya existentes como un archivo nuevo.)

Para documentos de texto: Los archivos de texto son muy propensos a gran cantidad de cambios de forma constante y cualquier cambio importante en su contenido suele dar paso un archivo nuevo.

- *Por primera vez o con 0 archivos nuevos semanales realizar un solo respaldo completo.*
- *De 1 a 20 archivos nuevos semanales realizar un respaldo incremental trimestral.*
- *De 21 a 50 archivos nuevos semanales realizar un respaldo incremental mensual.*
- *De 51 a 100 archivos nuevos semanales realizar un respaldo diferencial quincenal.*
- *Más de 101 archivos nuevos semanales realizar un respaldo diferencial a la semana.*

Para documentos audiovisuales: Su naturaleza de cambio en entornos no especializados es mucho menor a los archivos de solo texto.

- *Por primera vez o con 0 archivos nuevos semanales realizar un solo respaldo completo.*
- *De 1 a 5 archivos nuevos semanales realizar un respaldo incremental semestral.*
- *De 6 a 10 archivos nuevos semanales realizar un respaldo incremental bimensual.*
- *De 11 a 20 archivos nuevos semanales realizar un respaldo diferencial mensual.*
- *De 20 a 50 archivos nuevos semanales realizar un respaldo diferencial quincenal.*
- *50 o más archivos nuevos semanales realizar un respaldo diferencial a la semana.*

5.6.4.- Movilidad de la información digital:

Para casos en los que la movilidad de la información digital es necesaria hay varios dispositivos distintos con ventajas únicas en aspectos como tamaño, capacidad, consumo de energía, compatibilidad con distintos dispositivos, es difícil decir que un dispositivo para movilidad de información digital es mejor o peor que otro sin conocer la necesidad de la UI.

Daremos unas sugerencias concretas para algunos casos específicos que puedan adaptarse a varias necesidades que pueda presentar una UI.

Para información con recopilación y uso fuera de una sede de la UI se recomienda el uso de unidades USB y cualquiera de la serie SD (mini, micro).

Son utilizadas como estándares en equipos como laptops, tablets y celulares

- *Son dispositivo con soporte para lectura y escritura de datos, removibles lo que nos da un gran campo de acción en planes para movilidad de la información digital.*

Para resguardo y uso en sedes de la UI donde no se hará uso de la información más que en sitios preparados para ello (oficinas, aulas, casas, apartamentos) puede hacerse uso de unidades ópticas como CD, DVD y BlueRay, pero se recomienda el uso de discos duros portátiles de preferencia de estado sólido (SSD).

- *Ofrecen mayor protección contra daños por caídas o golpes.*
- *Muchos computadores nuevos no disponen de unidades lectoras para discos ópticos.*
- *Poseen mayor capacidad de almacenamiento que un disco óptico.*
- *Velocidad de lectura mayor.*

5.6.5.- Antivirus:

En el mercado podremos encontrar posiblemente miles de programas que ofrezcan dar la mejor protección a nuestro sistema pero, no todos son lo que realmente dicen, siempre de tiempo en tiempo habrá 3 o 4 antivirus que dominen el mercado, sin embargo hay varios aspectos importantes a evaluar al comprar o instalar un antivirus.

- *Cantidad de recursos del sistema que hace falta para que pueda ejecutarse.*
- *Capacidad de detección de virus.*
- *Actualización de la base de datos de virus conocidos.*
- *Velocidad de ejecución.*
- *Utilidades adicionales.*
- *Costo.*

Todas estas características son básicas al evaluar que antivirus necesita la UI pero, el análisis concreto lo debe dar un especialista dentro de la UI que conozca la necesidad de la UI al momento, algunos ejemplos.

Una UI pequeña con información personal privada: puede dar prioridad al costo, actualización del antivirus y velocidad de ejecución por disponer de menor presupuesto general y solo un computador que debe estar disponible mientras se preste servicio. Usando un antivirus open Access simple que detecte los virus más comunes.

Una UI mediana con información en la que recae el derecho de autor: puede dar prioridad a la detección de virus y al costo sobre los recursos que consuma el sistema al hacer un análisis pues dispone de más de un computador para atención al público. Usando un antivirus Open Access con posibilidades de pago con análisis más detallados y a su vez más prolongados ofreciendo una mejor protección.

Una UI de gran tamaño posiblemente de un ente privado que cobra por su servicio podría dar prioridad a la detección, actualización y opciones adicionales sobre el costo y recursos usando un antivirus pago de mayor calidad. Comprando una licencia de un antivirus reconocido con análisis regulares y análisis heurísticos para ofrecer mayor campo de detección y con sistemas integrados que evitan su propagación en la red interna de la UI o a dispositivos externos que se conecten al computador afectado.

5.6.6.- Estudio de Metadatos de preservación:

El aprender y capacitar al personal de las UI sobre la información que proporcionan los metadatos de preservación de los archivos digitales puede permitirnos detectar modificaciones no autorizadas, reforzar los procedimientos de revisión o auditorias de una institución, verificar la autenticidad de una imagen o un audio, verificar la autoría de un documento digital o incluso detectar elementos de plagio.

5.6.7.- Emulación:

Mucho se habla y se practica de la protección de archivos de texto, imágenes, audio y video, pero debemos recordar que el software tiene cualidades informativas que también deben ser protegidas, de ser posible en su totalidad.

Por ello la emulación de sistemas es considerado una de las mejores herramientas para recrear un software normalmente más antiguo o incompatible con cierto hardware en sistemas de uso recurrente o común, entre los casos más comunes encontramos:

Los emuladores enfocados en recrear un hardware en desuso, usualmente descontinuado como en el caso de consolas o máquinas recreativas.

Los emuladores de software que tienen como objetivo replicar el uso de un software no compatible en otro (usualmente un sistema operativo). Para los que podemos usar una máquina virtual

El uso de emuladores aun cuando es muy práctico para la protección existencial del software como información todavía tiene muchos vacíos legales no contemplados en algunas leyes internacionales, por lo cual se recomienda una asesoría legal dependiendo del software que se desee proteger.

CONCLUSIONES

Al observar los paradigmas de la bibliotecología en sus etapa física, cognitiva y social era notable la ausencia de procesos específicos para la protección de la información a un nivel intangible a largo plazo, se observó que los esfuerzos a lo largo de los distintos paradigmas de la bibliotecología son bastante consistentes pero todavía insuficientes para adaptarse 100% a las nuevas tecnologías. Sin embargo, herramientas como el uso de palabras clave para la recuperación de la información y operadores booleanos aplicados a los sistemas de recuperación de información han probado su efectividad ya que normalmente los sistemas nuevos se adaptan a estas herramientas.

En la protección de la información hay dos vertientes muy importantes y notablemente diferentes, las referidas al acceso y las referidas a la conservación

Dentro de los factores de riesgo se encuentran por supuesto muchos de los más naturales y comunes como: factores legales, el factor humano y la incidencia del ambiente en el soporte. Estos son factores de los que ya se tienen procedimientos que si bien no serían exactamente iguales, son fácilmente adaptables a la realidad digital. Hay otros que quizás no se han estudiado a fondo en el paradigma actual de la bibliotecología, como lo es la obsolescencia tecnológica, problemas específicos de hardware y cómo estos podrían afectar al software y viceversa.

Hay que ser conscientes sobre el hecho de que no hay una protección que sea cien por ciento efectiva y que el diseño de lineamientos, políticas, manuales o cualquier documento con sugerencias en procedimientos para la protección de la información de todo tipo es un campo de la investigación de los profesionales de la información a la que no se le permite un descanso pleno. De la misma forma como la tecnología avanza a pasos exponenciales, debe avanzar la investigación sobre la protección de la información que esa tecnología genere o resguarde.

Asimismo, con la tecnología que tenemos a la disposición la información digital es un recurso dominado en más de la mitad del mundo y por ello se debería tener el mayor cuidado posible. Quizás se deberían ramificar los estudios de seguridad de información digital en dos partes: la conservación en el tiempo de esa información y la protección en materia de acceso a la información, evaluar el alcance de las políticas de privacidad y confidencialidad versus el derecho a estar informado.

En muchos casos se subestima la facilidad de reproducción digital para aprovechar el uso de distintos tipos de almacenamiento como la nube, discos externos y servidores, entre otros, y cómo ayuda esto a crear respaldos periódicos, a medir cual es la mejor solución en el aspecto de seguridad basado en la relación costo/eficiencia y maximizar el uso del recurso humano del que disponga la institución; todo esto siempre que esté dentro de la normativa legal en curso.

RECOMENDACIONES

Para que los lineamientos acá presentados tengan una mayor incidencia, se debe hacer un estudio más a fondo de las necesidades y virtudes del paradigma actual de la bibliotecología. Esto se debe hacer en primera instancia por instituciones nacionales dado a que las necesidades de cada país pueden diferir, así como las fortalezas y debilidades.

Atacar los problemas de error humano en primera instancia ya que se estima tiene un menor costo y mayor provecho, luego apoyado por diferentes organizaciones internacionales conciliar el diseño de normas de acceso a la información verdaderamente transparentes sin limitación de ningún tipo para ningún grupo, apoyado en leyes de derecho internacional y que ataquen los principales factores de pérdida de información digital en áreas más técnicas como el encriptado y programación de protocolos de transmisión de datos en la web para seguridad en la nube.

Entrenar a los usuarios digitales sobre la importancia del uso de etiquetas y palabras claves para evitar duplicidad no programada de información, de igual forma crear campañas de capacitación tecnológica en cada herramienta que deban manejar los profesionales de la información para difundir contenido oportuno y acertado de las capacidades de cada herramienta. Esto puede darnos ventajas como mejoras en políticas de seguridad ideadas por los mismos profesionales en el área a cargo del resguardo de la información de todo ente, así esta sea de libre distribución o de carácter confidencial.

Buscar formas de disminuir la dificultad para acceder al contenido pertinente, crear planes de instrucción y capacitación a todo usuario de internet para que aprenda a depurar información en los buscadores y realice búsquedas efectivas, e instruir sobre los comandos de búsqueda específicos.

La cantidad de ruido e información repetida en internet es un factor que nos hace perder tiempo en investigaciones algo que nos puede traer consecuencias como encontrar una información cuando ya no sea oportuna o ser menos competitivos en ofrecer un servicio de

recuperación de información. Es un proceso que puede ser largo y engorroso pero nos permitiría ser profesionales de la información capaces de aprovechar al máximo los contenidos disponibles en la red sin emplear servicios de terceros.

Con apoyo de instituciones internacionales en cumbres de la sociedad de la información se sugiere crear una tabla de clasificación de confidencialidad con carácter internacional para facilitar el manejo y resguardo en el ambiente digital global.

BIBLIOGRAFÌA

Aguilar Castillo, Gildardo [sin fecha] *Delitos informáticos* [pdf en línea] Universidad Veracruzana, México. Disponible en: http://www.oocities.org/mx/academia_entorno/eli4.pdf [Consultado el 06/09/2013]

ALCTS (2013) *Microforms in Libraries and Archives* [web en línea] American Library Association, EEUU. Disponible en: http://www.oocities.org/mx/academia_entorno/eli4.pdf [Consultado el 20/07/2015]

Apolín Meza, Dante (2012) *LOS PROBLEMAS DE LA ORALIDAD EN EL PROCESO CIVIL* [Blog] Perú. Disponible en: http://www.ius360.com/articulos/derecho-procesal/2012/02/los-problemas-de-la-oralidad-en-el-proceso-civil [Consultado el 11/07/2013]

ASLIB (1966) *Factors determining the performance of indexing systems volume I design* [pdf en línea] National Science Foundation, Cranfield. Disponible en: http://www.sigir.org/museum/pdfs/Factors%20Determining%20the%20Performace%20of%20Indexing%20Systems%20Vol%201%20-%20Part%201%20Text/pdfs/ [Consultado el 03/06/2013]

ASLIB (1966) *Factors determining the performance of indexing systems chapter 1*[pdf en línea] National Science Foundation, Cranfield. Disponible en: http://www.sigir.org/museum/pdfs/Factors%20Determining%20the%20Performace%20of%20Indexing%20Systems%20Vol%201%20-%20Part%201%20Text/pdfs/p1-chapter_1.pdf [Consultado el 03/06/2013]

ASLIB (1966) *Factors determining the performance of indexing systems chapter 2* [pdf en línea] National Science Foundation, Cranfield. Disponible en: http://www.sigir.org/museum/pdfs/Factors%20Determining%20the%20Performace%20of%20Indexing%20Systems%20Vol%201%20-%20Part%201%20Text/pdfs/p9-chapter_2.pdf [Consultado el 03/06/2013]

ASLIB (1966) *Factors determining the performance of indexing systems chapter 3* [pdf en línea] National Science Foundation, Cranfield. Disponible en: http://www.sigir.org/museum/pdfs/Factors%20Determining%20the%20Performace%20of%20Indexing%20Systems%20Vol%201%20-%20Part%201%20Text/pdfs/p19-chapter_3.pdf [Consultado el 03/06/2013]

ASLIB (1966) *Factors determining the performance of indexing systems chapter 4* [pdf en línea] National Science Foundation, Cranfield. Disponible en: http://www.sigir.org/museum/pdfs/Factors%20Determining%20the%20Performace%20of%20Indexing%20Systems%20Vol%201%20-%20Part%201%20Text/pdfs/p40-chapter_4.pdf [Consultado el 03/06/2013]

ASLIB (1966) *Factors determining the performance of indexing systems chapter 5* [pdf en línea] National Science Foundation, Cranfield. Disponible en: http://www.sigir.org/museum/pdfs/Factors%20Determining%20the%20Performace%20of%20Indexing%20Systems%20Vol%201%20-%20Part%201%20Text/pdfs/p58-chapter_5.pdf [Consultado el 03/06/2013]

ASLIB (1966) *Factors determining the performance of indexing systems chapter 6* [pdf en línea] National Science Foundation, Cranfield. Disponible en: http://www.sigir.org/museum/pdfs/Factors%20Determining%20the%20Performace%20of%20Indexing%20Systems%20Vol%201%20-%20Part%201%20Text/pdfs/p90-chapter_6.pdf [Consultado el 03/06/2013]

ASLIB (1966) *Factors determining the performance of indexing systems chapter 7* [pdf en línea] National Science Foundation, Cranfield. Disponible en: http://www.sigir.org/museum/pdfs/Factors%20Determining%20the%20Performace%20of%20Indexing%20Systems%20Vol%201%20-%20Part%201%20Text/pdfs/p106-chapter_7.pdf [Consultado el 03/06/2013]

Biblioteca Nacional de Australia (2003) *Directrices para la preservación del patrimonio digital* [pdf en línea] División de la sociedad de la información UNESCO. Disponible en: http://unesdoc.unesco.org/images/0013/001300/130071s.pdf [Consultado el 16/01/2013]

Cáceres, Pablo (2003) *Análisis cualitativo de contenido: una alternativa metodológica alcanzable* [pdf en línea] Pontificia Universidad Católica de Valparaíso, Chile. Disponible en: http://www.psicoperspectivas.equipu.cl/index.php/psicoperspectivas/article/viewFile/3/3 [Consultado el 07/04/2013]

Calderón, Andoni (2006) *Los documentos y sus clases* [pdf en línea] Universidad Autónoma Gabriel René Moreno, Bolivia. Disponible en: http://xa.yimg.com/kq/groups/84473624/473028916/name/los+documentos+y+sus+clases.pdf [Consultado el 24/01/2013]

Calderón Delgado, Marco A (2009) *Conservación Preventiva de Documentos* [pdf en línea] Archivo Nacional de Costa Rica, Costa Rica. Disponible en: http://www.archivonacional.go.cr/pdf/conservacion_preventiva_documentos.pdf [Consultado el 20/10/2012]

Campos Moraima, M; Auxiliadora Mujica, L (2008) *EL ANALISIS DE CONTENIDO: Una forma de abordaje metodológico* [pdf en línea] Laurus, Venezuela. Disponible en: http://redalyc.uaemex.mx/redalyc/pdf/761/76111892008.pdf [Consultado el 19/01/2013]

Capurro, Rafael (2010) *Epistemología y ciencia de la información* [portal web] Portal web, Alemania. Disponible en: http://www.capurro.de/enancib.htm[Consultado el 01/06/2013]

Carrion G, Hugo (2007) *Preservación de Información Digital* [pdf en línea] Pontificia Universidad Javeriana, Bogotá. Disponible en: http://www.imaginar.org/javeriana/index_archivos/presentacion.pdf [Consultado el 20/10/2012]

Clareth Bonilla, José (2000) *Epistemología, Sin Sujeto Cognoscente de Karl Popper* [pdf en línea] La reja en el aire, (Colombia). Disponible en: http://www.larejaenelaire.com/docs/fonteras/Epistemologia%20sin%20sujeto%20cognoscente.pdf [Consultado el 12/06/2013]

Codina, Lluis (2001) *Propiedades de la información digital*. [pdf en línea] Disponible en: http://infonautica.net/docs/infomag/infodigital/contenidos/textos/Codina.pdf [Consultado el 20/10/2012]

Consejo Internacional de Archivos (2005) *Documentos electrónicos: manual para archiveros* [pdf en línea] Ministerio de Cultura, España. Disponible en: http://www.mcu.es/archivos/docs/documentosElectronicos.pdf [Consultado el 19/01/2013]

Convervaplan (número 11, 1999) *LA RELACIÓN ENTRE LA TECNOLOGÍA DE CONVERSIÓN DIGITALY OTROS PROCESOS DECONVERSIÓN DE MEDIOS: GLOSARIO ESTRUCTURADO DE TÉRMINOS TÉCNICOS* [pdf en línea] Biblioteca Nacional de Venezuela, Caracas. Disponible en: http://www.bnv.gob.ve/pdf/Conser11.pdf [Consultado el 22/10/2012]

Convervaplan (número 7, 1998) *EL MANUAL DE PRESERVACIÓN DE BIBLIOTECAS Y ARCHIVOS DEL NORTHEAST DOCUMENT CONSERVATION CENTER* [pdf en línea] Biblioteca Nacional de Venezuela, Caracas. Disponible en: http://www.abinia.org/conser7-2.pdf [Consultado el 22/07/2015]

Del Mar Rosell, María (número 289, 2010) *La fragilidad de la memoria digital desafía a gestores y organizaciones* [pdf en línea] Técnica Industrial, España. Disponible en: http://www.tecnicaindustrial.es/TIAdmin/Numeros/74/792/a792.pdf [Consultado el 22/10/2012]

Deliberali Maimone, Giovana (2011) *La ciencia de la información en el contexto de la postmodernidad* [pdf en línea] Anales de documentación, Ediciones de la Universidad de Murcia, España. Disponible en: http://eprints.rclis.org/15490/1/Ad14%20Deliberali%20G%20Anales%20de%20Documentacion.pdf [Consultado el 30/05/2013]

Díaz Rodríguez, Alfonso (2007) *La validación de los documentos: pasado, presente y futuro* [pdf en línea] Principado de Asturias, España. Disponible en: http://ria.asturias.es/RIA/bitstream/123456789/56/1/02_Concepto_doc_electr_validacion.pdf [Consultado el 19/01/2013]

Dodson Cates, Suzanne (2001) *MICROFILM: STILL MY TOP CHOICE FOR A PRESERVATION MEDIUM* [web en linea] Microfilm Service Group, Vancouver, Canada. Disponible en: http://www.fyiglover.com/articles/preservation.html [Consultado el 20/07/2015]

Domínguez Mujica, Carmen (2003) *Sintaxis de la lengua oral Oralidad y escritura: dos objetos y una lengua* [pdf en línea] Universidad de Los Andes, Mérida, Venezuela. Disponible en: http://www.human.ula.ve/linguisticahispanica/documentos/Dominguez.pdf [Consultado el 11/07/2013]

Echaiz, Javier [sin fecha] *Teoría de la Información* (Extracto del libro: Introducción a la psicología de la comunicación) [pdf en línea] Universidad Nacional del Sur, Argentina. Disponible en: http://cs.uns.edu.ar/~ldm/data/ss/info/teoria_de_la_informacion2.pdf [Consultado el 03/06/2013]

Esteban Navarro, Miguel A (número 12 2001) *Los archivos de documentos electrónicos* [pdf en línea] El profesional de la información, Revista Internacional. Disponible en: http://www.elprofesionaldelainformacion.com/contenidos/2001/diciembre/9.pdf [Consultado el 19/01/2013]

Gallego González, Sofía (2009) *LA TEORÍA DE LAS INTELIGENCIAS MÚLTIPLES EN LA ENSEÑANZA-APRENDIZAJE DE ESPAÑOL COMO LENGUA EXTRANJERA* [pdf en línea] Universidad de Salamanca, España. Disponible en: http://gredos.usal.es/jspui/bitstream/10366/76442/1/DLE_Gallego_Gonzalez_S_Lateoriadelasinteligencias.pdf [Consultado el 26/06/2013]

García Marco, Francisco (1995) *Paradigmas científicos en representación y recuperación de la información* [pdf en línea] Facultad de Filosofía y Letras, Universidad de Zaragoza, España Disponible en: https://www.google.co.ve/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&ved=0CDsQFjAB&url=http%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F2341318.pdf&ei=PsKsUYKiAoXc9QThv4D4BQ&usg=AFQjCNF5N9dQk1UyL2nOiVFYI9ksb57H0g&sig2=fCYfXEozYm9Bc-0sDQWOhg&bvm=bv.47244034,d.eWU [Consultado el 03/06/2013]

García Testal, Cristina (1999) *Archivos digitales y conservación del documento* [artículo en línea] Resumen El profesional de la información, Revista Digital Internacional. Disponible en: http://www.elprofesionaldelainformacion.com/contenidos/1999/junio/archivos_digitales_y_conservacion_del_documento.html [Consultado el 25/10/2012]

Green Seal (2006) *Proposed Enviromental Standard and Evironmental Evaluation of Recycled-Content Latex Paint* [pdf en línea]. Green Seal. Disponible en: http://www.usgbc.org/Docs/News/News2285.pdf [Consultado el 01/12/2012]

Gómez Valencia, Herinaldy [sin fecha] *Justicias orales indígenas y sus tensiones con la ley escrita* [pdf en línea] Universidad de Cauca, Colombia. Disponible en: http://www.ciesas.edu.mx/proyectos/relaju/cd_relaju/Ponencias/Mesa%20Ortiz,%20H%C3%A9ctor/GomezValenciaHerinaldy.pdf[Consultado el 26/07/2013]

González Longatt, Francisco (2007) *Capítulo 2: definiciones y clasificación de la estabilidad* [pdf en línea] www.fglongatt.org/ (Venezuela). Disponible en: http://www.fglongatt.org/Archivos/Archivos/SP_II/PPTCapitulo2SP2.pdf [Consultado el 03/07/2013]

Goñi Camejo, Ivis (2000) *Algunas reflexiones sobre el concepto de información y sus implicaciones para el desarrollo de las ciencias de la información* [pdf en línea] ACIMED, Cuba. Disponible en: http://bvs.sld.cu/revistas/aci/vol8_3_00/aci05300.pdf [Consultado el 19/01/2013]

Hernández, Edecia (2012) *Sistema de Gestión de documentos, Tecnologías e Interoperabilidad: Tres aspectos manifiestos en el contexto de las Ciencias de la Información.* [pdf en línea] Saber UCV, Venezuela. Disponible en: http://saber.ucv.ve/jspui/handle/123456789/4676 [Consultado el 22/07/2015]

Hernández Sampieri, R; Fernández Collado, C; Baptista Lucio, P. (2003) *METODOLOGÍA DE LA INVESTIGACIÓN* [pdf en línea] MCGRAW-HILL, México. Disponible en: http://www.dgsc.go.cr/dgsc/documentos/cecades/metodologia-de-la-investigacion.pdf [Consultado el 01/02/2013]

Hernández Quintana, Ania. (2007) *Paradigmas dominantes y emergentes en la Bibliotecología y la Ciencia de la Información: continuidad y ruptura en la dinámica informacional.* [Portal web] Acimed, Biblioteca virtual en salud, Cuba. Disponible en: http://bvs.sld.cu/revistas/aci/vol16_3_07/aci02907.html [Consultado el 01/06/2013]

Hilbert, Martin; López, Priscila (2011) *The World's Technological Capacity to Store, Communicate, and Compute Information* [pdf en línea] www.sciencexpress.org/ (EEUU) . Disponible en:http://www.ris.org/uploadi/editor/13049382751297697294Science-2011-Hilbert-science.1200970.pdf [Consultado el 22/04/2015]

Hilde Van Wijngaarden (2008) *Preservation Action: What, how and when?* [pdf en línea] National Library of the Netherlands, Países Bajos. Disponible en:

http://www.planets-project.eu/docs/presentations/Planets_Tools-and-Trends_HildeVanWijngaarden.pdf [Consultado el 19/01/2013]

IFLA (número 24, 2008) *Newsletter* [pdf en línea] IFLA, Canadá. Disponible en: http://www.ifla.org/files/assets/preservation-and-conservation/newsletters/s19-newsletter-2008-07-es.pdf [Consultado el 16/01/2013]

IFLA (2010) *La conservación y preservación de la documentación digital en las bibliotecas especializadas de la generalidad de Cataluña* [pdf en línea] IFLA, España. Disponible en: http://www.ifla.org/files/assets/government-libraries/ConferencePapers/2010Barcelona-Heideprem-Spanish3.pdf [Consultado el 16/01/2013]

Imaginar (2004). *Manual de digitalización* [pdf en línea]. Information & Image Management Systems, S.A. Disponible en: http://www.imaginar.org/dgd/manuales/manual_digitalizacion.pdf [Consultado el 10/12/2012]

Jiménez Rosano, Cristina M (2005) *El ensayo fotográfico como diseño de información* [pdf en línea] Universidad de las Américas Puebla, México .Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/ldf/jimenez_r_mc/capitulo1.pdf [Consultado el 24/01/2013]

Jiménez Delgadillo, Gloria A (2013) *ADQUISICIÓN DEL CONOCIMIENTO A PARTIR DEL PROCESAMIENTO DE INFORMACIÓN* [pdf en línea] Blog Wordpress, .Disponible en: https://karenvihu.files.wordpress.com/2013/06/adquisicion-de-conocimiento-1.pdf [Consultado el 21/07/2015]

Popper, Karl (1978) *Three Worlds* [pdf en línea] Universidad de Michigan. EEUU. Disponible en: http://tannerlectures.utah.edu/_documents/a-to-z/p/popper80.pdf [Consultado el 22/07/2015]

KODAK [2015] *Photography* [web en línea] KODAK, España .Disponible en: http://graphics.kodak.es/ES/es/corp/aboutus/heritage/photography/default.htm [Consultado el 20/07/2015]

Lamson, Stephanie (2015) *Preservation Reformatting and Replacement* [pdf en línea] Unive rsidad de Washington, Washington, EEUU. Disponible en: https://www.google.co.ve/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0CD8QFjAEahUKEwiS7tmEk-vGAhWB1x4KHQveAus&url=https%3A%2F%2Fcanvas.uw.edu%2Fcourses%2F966673%2Ffiles%2F31607944%2Fdownload%3Fverifier%3DXUOuhgvL9SssXoXnau1AR0oHm6TJONlBd11nWu5o%26wrap%3D1&ei=nKqtVZKwLoGve4u8i9gO&usg=AFQjCNGqEexIymepMDwehD02X05FStX1bQ&sig2=yqg574sER14UCiP4-phkSA [Consultado el 20/07/2015]

Lehembre, Guillaume (2009) *Seguridad Wi-Fi – WEP, WPA y WPA2* [pdf en línea] Hakin9 IT security Magazine. Disponible en: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf [Consultado el 02/07/2013]

Lelis García, Hilda; Mireles Cárdenas, Celia (2002) *APORTACIONES DE PAUL OTLET A LA BIBLIOTECOLOGÍA ACTUAL* [pdf en línea] LIBER: revista de Bibliotecología de AMBAC, México. Disponible en: http://eprints.rclis.org/6133/1/mireles.pdf [Consultado el 20/06/2013]

Linares Columbié, Radamés (2010) *Epistemología y Ciencia de la Información: repensando un diálogo inconcluso* [pdf en línea] ACIMED. Cuba. Disponible en: http://eprints.rclis.org/15104/1/Epistemolog%C3%ADa_y_Ciencia_de_la_Informaci%C3%B3n.pdf [Consultado el 16/06/2013]

LSI soluciones (2014) *Diferencis entre discos duros SATA, SAS y SSD* [web en línea] Laboratorio de sistemas informáticos, España. Disponible en: [Consultado el 23/07/2015]

Luminous Lint [sin fecha] *John Benjamín Dancer* [html en línea] Luminous Lint. Disponible en: http://www.luminous-lint.com/app/photographer/John_Benjamin__Dancer/A/ [Consultado el 22/10/2012]

Mansilla, Lizama, Gutarra y Rodríguez (2012) *Tratamiento de Residuos Líquidos de la Industria de celulosa y textil* [pdf en línea] Plataforma Solar de Almería, España. Disponible en: http://www.psa.es/webeng/solwater/files/CYTED01/20cap13.pdf [Consultado el 22/10/2012]

Massone Moya, Francisca (2006) *PEDRO URDEMALES Y LA EXPERIENCIA DE LA ORALIDAD EN EL CAMPO CHILENO DEL SIGO XIX* [pdf en línea] Revista de Antropología Social, Universidad de Chile, Santiago, Chile. Disponible en: http://myslide.es/download/document/?id=Kbki2q%2FvS%2BH%2Fy4OA3xTfWT9MVypbOcwql4fedwpAgbaAdqZr%2B16NPZAY3%2BIu6PQXXWh2UHzsr7Qq5pzVnBMvaA%3D%3D [Consultado el 07/08/2013]

Marcos, Mari C (1999) *Los archivos en la era digital* [pdf en línea] El profesional de la información, Revista científica internacional. Disponible en:

http://aplicacionesarchivos.weebly.com/uploads/1/3/7/7/13775799/lectura_05.pdf [Consultado el 07/08/2014]

Martinez Navarro, Germàn (2011) *La máquina enigma y otros dispositivos de encriptación* [pdf en línea] Universitat de Valencia, España. Disponible en: http://www.uv.es/~montanan/redes/trabajos/enigma.pdf [Consultado el 07/08/2014]

Ministerio de Cultura de España (1988) *Principios para la preservación y conservación de los materiales bibliográficos* [pdf en línea] Dirección General del Libro y Bibliotecas, Madrid. Disponible en: http://web.usal.es/~alar/Bibweb/Temario/Dureau.PDF [Consultado el 22/10/2012]

Monsonyi, Esteban (1990) *Oralidad: ANUARIO PARA EL RESCATE DE LA TRADICIÓN ORAL DE AMÉRICA LATINA Y DEL CARIBE* [pdf en línea] UNESCO, La Habana, Cuba. Disponible en: http://www.lacult.org/docc/oralidad_02_5-19-la-oralidad.pdf [Consultado el 11/07/2013]

Montero Aroca, Juan (1994) *La herencia procesal Española* [pdf en línea] UNAM, México. Disponible en: http://biblio.juridicas.unam.mx/libros/1/199/6.pdf [Consultado el 26/07/2013]

Mundoarchivistico.com (2011) La fragilidad de los archivos digitales. Una mesa sobre los desafíos de archivar los medios digitales [blog en línea] Mundoarchivistico.com. Disponible en: http://www.mundoarchivistico.com.ar/?menu=noticias&accion=ver&id=1208 [Consultado el 29/10/2012]

NACIONES UNIDAS (1960) *Treaties and international agreements registered or filed and recorded with the Secretariat of the United Nations* [pdf en línea] UNITED NATIONS TREATY COLLECTION Disponible en: http://treaties.un.org/doc/Publication/UNTS/Volume%20375/v375.pdf [Consultado el 20/06/2013]

National Diet Library (2006) *The Long-term Accessibility of Packaged Digital Publications* [pdf en línea] National Diet Library, Japón. Disponible en: http://www.ndl.go.jp/en/aboutus/pdf/report_no6.pdf [Consultado el 16/01/2013]

Nieva Fenoll, Jordi (2010) *LOS PROBLEMAS DE LA ORALIDAD* [pdf en línea] Associação do Ministério Público do Rio Grande do Sul (AMP/RS), Brasil. Disponible en: http://www.amprs.org.br/arquivos/revista_artigo/arquivo_1303931237.pdf [Consultado el 11/07/2013]

Nigro, Patricia (2012) *Modelo de comunicación de Shannon y Weaver* [pdf en línea] Facultad de Comunicación de la Universidad de Austral, Argentina. Disponible en: http://catedralengua1.files.wordpress.com/2012/03/modelo-de-comunicacic3b3n-de-shannon-y-weaver.pdf[Consultado el 01/06/2013]

Pérez Moya, Felicia (2011) *Bibliotecología y estudios culturales: elementos teóricos que posibilitan su vinculación* [pdf en línea] Anales de investigación, Biblioteca nacional de Cuba José Martí, Cuba. Disponible en: http://anales.bnjm.cu/bundles/anales/dossiers/2011/1Felicia_Perez_Moya.pdf[Consultado el 01/06/2013]

Pollock, Neil (2002) *Birger Hjorland 101* [pdf en línea] University of Technology, Sydney. Disponible en: http://npollock.id.au/info_science/hjorland.pdf[Consultado el 01/06/2013]

PREMIS (2010) *PREMIS data dictionary, versión 2.0* [pdf en línea] Library of Congress, Estados Unidos. Disponible en: http://www.loc.gov/standards/premis/PREMIS_es.pdf [Consultado el 11/06/2015]

PricewaterhouseCoopers (2012) *Más allá de las amenazas cibernéticas: El primer Índice de Madurez del Riesgo de la Información en Europa* [pdf en línea] PWC, Reino Unido. Disponible en: http://www.ironmountain.es/~/media/910459DC0CC948AA9D63AA28D393377F.pdf [Consultado el 27/08/2013]

PROQUEST [1996] *History & Milestones* [web en línea] PROQUEST, Reino Unido. Disponible en: http://www.proquest.com/about/history-milestones/ [Consultado el 20/07/2015]

PwC [2014] *Executive summary* [pdf en línea] Iron Mountain, Reino Unido. Disponible en: http://www.ironmountain.co.uk/~/media/Files/Iron%20Mountain/Knowledge%20Center/Reference%20Library/Europe/White%20Papers/P/PwC%20Executive%20summary.ashx?la=en-GB/ [Consultado el 20/07/2015]

Recovery Labs (2003) *Principales factores que causan una pérdida de información* [pdf en línea] Recovery Labs, España. Disponible en: http://www.recoverylabs.com/informes/Recovery_Labs_Factores.pdf[Consultado el 27/08/2013]

Richarte, Javier (2011) *Técnico Hardware: Las más novedosas soluciones en reparación de PC: Problemas de inestabilidad* [pdf en línea] REDUSERS, MP Ediciones, Argentina. Disponible en: http://es.scribd.com/doc/73017962/inestabilidad-de-PC[Consultado el 03/07/2013]

Rivas López, José Luis (2003) *Protección de la información* [pdf en línea] Ediciones VirtuaLibro. Disponible en: http://webs.uvigo.es/jlrivas/downloads/publicaciones/protinf.pdf [Consultado el 20/10/2012]

Riviere, Angel (1991) *Orígenes históricos de la psicología cognitiva: paradigma simbólico y procesamiento de la información* [pdf en línea] Universidad Autónoma de Madrid, E spaña. Disponible en: http://u.jimdo.com/www16/o/s98d61c8552d4a915/download/m508c01845f96519c/1430924939/Origenes+Historicos.pdf [Consultado el 20/10/2012]

Rodríguez García, Ariel A (2010) *Las nuevas entidades de información analizadas desde la perspectiva de la organización de la información* [pdf en línea] Universidad Autónoma de México, México. Disponible en: http://libros.metabiblioteca.org/bitstream/001/221/9/978-607-02-1420-2.pdf [Consultado el 19/01/2013]

Rodríguez R, Sulema (2007) *El análisis de dominio en la ciencia de la información* [pdf en línea] ECIMED, Cuba. Disponible en: http://scielo.sld.cu/pdf/aci/v15n6/aci07607.pdf [Consultado el 16/06/2013]

Romero, María A (2013) *LA ORALIDAD COMO FORMA POSIBLE DE CONSTRUCCIÓN DEL CONOCIMIENTO* [pdf en línea] Cuadernos de la Facultad de Humanidades y

Ciencias Sociales, Universidad Nacional de Jujuy, Argentina. Disponible en: http:// www.redalyc.org/pdf/185/18532860007.pdf [Consultado el 22/07/2015]

Salazar Solis, Carlos (2012) *masificando el conocimiento en seguridad de la información* [blog] Disponible en: http://www.solis.com.ve/5-cosas-que-tienes-que-saber-sobre-seguridad-de-servidores/ [Consultado el 06/09/2013]

Sampieri Hernández, R; Fernández Collado, C; Baptista Lucio, P (1997) *Metodología de la investigación* [pdf en línea] McGraw Hill, México. Disponible en: http://www.upsin.edu.mx/mec/digital/metod_invest.pdf [Consultado el 16/01/2013]

Santillan Rivero, E (2008) *Guía para el uso y cuidado de los libros*. [pdf en línea]. Centro de investigación y de estudios avanzados del I.P.N. Biblioteca Cinvestav, Querétaro, México. Disponible en: http://www.qro.cinvestav.mx/docs/biblioteca/guiasyman/gym02.pdf [Consultado el 20/11/2012]

Sanjuán Pérez, Antonio S (2001) *Marketing y comercialización de información documental electrónica* [pdf en línea] Universidad Complutense de Madrid, España. Disponible en: http://eprints.ucm.es/tesis/inf/ucm-t25159.pdf [Consultado el 19/01/2013]

SAPI [s/f]a *Derecho de autor* [web en línea] Servicio Autónomo de la Propiedad Intelectual, Venezuela. Disponible en: http://www.sapi.gob.ve/?q=preguntas_derecho [Consultado el 22/07/2015]

SAPI [s/f]b *Patentes* [web en línea] Servicio Autónomo de la Propiedad Intelectual, Venezuela. Disponible en: http://www.sapi.gob.ve/?q=preguntas_patentes [Consultado el 22/07/2015]

SECOMDATA (2009) *Qué es el cifrado (encriptación)* [web en línea] Mobile High Security, España. Disponible en: http://www.secomdata.com/qu%C3%A9-es-el-cifrado-encriptaci%C3%B3n/ [Consultado el 24/01/2013]

Serra Serra, Jordi (2001) *Gestión de los documentos digitales: estrategias para su conservación* [pdf en línea] El profesional de la información, Revista Digital Internacional. Disponible en: http://diposit.ub.edu/dspace/bitstream/2445/24347/1/525913.pdf [Consultado el 24/01/2013]

Singhal, Amit (2001) *Modern Information Retrieval: A Brief Overview* [pdf en línea] Disponible en: http://singhal.info/ieee2001.pdf [Consultado el 03/06/2013]

SRLF (2001) *MICROFILM - A BRIEF HISTORY* [web en línea] Universidad de California, Los Angeles. Disponible en: http://www.srlf.ucla.edu/exhibit/text/BriefHistory.htm [Consultado el 20/05/2014]

SUSCERTE (2007) *Uso de los Certificados Uso de los Certificados Electrónicos y Firma Electrónica* [pdf en línea] Ministerio para el Poder Popular para las Telecomunicaciones y la Informática, Caracas. Disponible en: http://ldc.usb.ve/~figueira/Cursos/Seguridad/Material/PKI-gmoline.pdf [Consultado el 20/07/2015]

Tramullas, Jesús (2003) *Diseño centrado en el usuario de servicios de información digital* [pdf en línea] Dpto. Ciencias de la documentación Univ. de Zaragoza, España. Disponible en: http://infonautica.net/docs/infomag/gescon/contenidos/textos/Tramullas_2.pdf [Consultado el 20/10/2012]

Tripaldi, Nicolás (2010) *Desarrollo profesional de los bibliotecólogos en las organizaciones: transdisciplina y profesionalismo* [pdf en línea] INTA. Biblioteca y Archivo Documental, Argentina. Disponible en: http://eprints.rclis.org/15151/1/Ponencia_Desarrollo_Profesional_-_Tripaldi.pdf [Consultado el 12/06/2013]

Turner, Fay (2010) *AN OVERVIEW OF THE Z39.50 INFORMATION RETRIEVAL STANDARD* [pdf en línea] National Library of Canada. IFLA, Canada. Disponible en: http://www.ifla.org/archive/udt/op/udtop3/udt-op3.pdf [Consultado el 12/06/2013]

UNESCO (2013) *Textos fundamentales de la Convención de 2005 sobre la Protección y la Promoción de la Diversidad de las Expresiones Culturales* [pdf en línea] Sección de la Diversidad de las Expresiones Culturales Sector de la Cultura, Francia. Disponible en: http://unesdoc.unesco.org/images/0022/002253/225383S.pdf [Consultado el 20/07/2015]

UNOCERO (2008) *Intel core i7 las pruebas* [web en línea] Servicios Track Cero, S.C, Mexico. Disponible en: https://www.unocero.com/2008/11/17/intel-core-i7-las-pruebas/ [Consultado el 20/07/2015]

USERS (2010) *REDUSERS DESDE CERO: Introducción a los problemas de la PC* [pdf en línea] MP Ediciones, Argentina. Disponible en: http://img.redusers.com/imagenes/libros/lpcu108/capitulogratis.pdf [Consultado el 03/07/2013]

Van Der Hoeven, J; Van Wijngaarden, H (2005) *Modular emulation as a long-term preservation strategy for digital objects* [pdf en línea] National Library of the Netherlands, Países Bajos. Disponible en: http://iwaw.europarchive.org/05/papers/iwaw05-hoeven.pdf [Consultado el 16/08/2014]

Van Dormolen; Gillesse Robert (2007) *Metamorfoze Preservation Imaging Guidelines* [pdf en línea] National Library of the Netherlands, Países Bajos. Disponible en: http://www.metamorfoze.nl/sites/metamorfoze/files/bestanden/richtlijnen/guidelinespijune07.pdf [Consultado el 16/01/2013]

Vargas Q, Benjamín; De Moya Anegon, Félix; Olvera Lobos, María (2002) *Enfoques en torno al modelo cognitivo para la recuperación de información: análisis crítico* [pdf en línea] Departamento de Biblioteconomía y Documentación Facultad de Biblioteconomía y Documentación, Universidad de Granada, España. Disponible en: http://www.scielo.br/pdf/ci/v31n2/12914.pdf [Consultado el 12/06/2013]

Vega Almeida, Rosa (2010) *Ciencia de la información y paradigma social: Enfoques histórico, epistemológico y bibliométrico para un análisis de dominio* [pdf en línea] Universidad de Granada, España. Disponible en: http://digibug.ugr.es/bitstream/10481/15418/1/19565859.pdf [Consultado el 16/06/2013]

Velduque Ballarín, Maria, J (2011) *El origen de la imprenta: la xilografía. La imprenta de Gutenberg* [pdf en línea] Revista de Claseshistoria, Toledo, España. Disponible en:

http://www.claseshistoria.com/revista/2011/articulos/velduque-imprenta-origen.pdf [Consultado el 21/07/2015]

Vidal Gil, Jesús (2006) *Un método general, sencillo y eficiente, para la definición y simulación numérica de sistemas multicuerpo* [pdf en línea] Universidad Politécnica de Madrid, España. Disponible en: http://oa.upm.es/462/1/JESUS_VIDAL_GIL.pdf[Consultado el 02/07/2013]

Websense (2008) *Protección de la información esencial* [pdf en línea] Websense, Internacional. Disponible en: http://www.websense.com/assets/white-papers/whitepaper_protecting_essential_information_es.pdf [Consultado el 20/10/2012]