PRESERVACION DOCUMENTAL DIGITAL
Y SEGURIDAD INFORMATICA

NANCY JANETH HERNANDEZ CONTRERAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BASICAS TECNOLGIAS E INGENIERIAS
PROYECTO DE SEGURIDAD INFORMATICA
COROZAL
2021

PRESERVACION DOCUMENTAL DIGITAL Y SEGURIDAD INFORMATICA

NANCY HERNANDEZ CONTRERAS

Trabajo monográfico para optar por el título de Especialista en Seguridad informática

ING. MARTIN CAMILO CANCELADO
ING. YENNY STELLA NUÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BASICAS TECNOLGIAS E INGENIERIAS
PROYECTO DE SEGURIDAD INFORMATICA
COROZAL
2021

NOTA DE ACEPTACION

_____

_____

_____

_____

PRESIDENTE DEL JURADO

_____

JURADO 1

_____

JURADO 2

COROZAL 28 de abril de 2020 **fecha de entrega**

CONTENIDO

Pág.

LISTA DE FIGURAS

TABLAS

GLOSARIO

CONFIDENCIALIDAD DE LOS DATOS. Son todas las copias en secreto definidas solo por los usuarios con autenticación para ocultar y abrir su contenido, de ahí los documentos copiados solo son para un grupo personas con autenticación definida por su gerente administrativo.

DATOS. Caracteres que encadenados ordenadamente dan sentido a la información.

DOCUMENTOS. Son todos los archivos que conforman un libro de tal manera que se distinguen al manipular sus temas destinados de los usuarios dependiendo de conocimiento y sus fines de autenticación y protección de datos.

FORMATO ALMACENAMIENTO. Todo tipo de programa que admite un conjunto de datos de diferentes copias, sean imágenes digitales o archivos según los propósitos de los datos de protección.

PRESERVACION DE DATOS. Las diferentes autenticaciones que se emplean para evitar corromper el contenido de la degradación de las copias documentales.

SEGURIDAD DE LA INFORMACION. Se comprende como el conjunto de requisitos que se deben seguir para la precaución con el fin de evitar que se pierda la información o datos de un servidor o de un sistema informático en general.

RESUMEN

La información es uno de los activos más importantes para cualquier entidad, sin embargo, algo que parece fácil manejar se ha vuelto complejo debido a la creciente demanda de información que día a día se acumula sin contar con los espacios requeridos y complicando luego su búsqueda, además, en la constante y rápida evolución de la tecnología se ha visto afectada su permanencia poniendo en riesgo su pérdida total, teniendo en cuenta que muchos no han seguido las debidas acciones ya sea por falta de conocimientos, por los avances tecnológicos surjan nuevas versiones, que la compatibilidad entre los formatos y los dispositivos sea nula haciendo difícil el mantener dicha información, por eso es necesario dar a conocer los diferentes métodos de almacenamiento y brindar las mejores opciones para que se mantengan seguros aquellos documentos de mucha importancia para un usuario, lo cual se lograría a través de actualizaciones y copias de seguridad por medio de soportes confiables con la capacidad de mantener y migrar información en un futuro.

Además de los medios de almacenamiento disponibles para guardar contenidos digitales electrónicos también existen metodologías que ayudan a establecer políticas de seguridad en los sistemas informáticos con el fin de mantener la disponibilidad, confidencialidad e integridad de los datos que se procesan en las organizaciones.
Por esto se mencionarán algunas metodologías que mediante practicas ayudarán a mantener y resguardar la información de manera que se pueda actuar frente a los riesgos y amenazas que esta pueda sufrir, facilitando la permanencia y la accesibilidad sin importar el tiempo que pase.

Palabras clave: Archivos, backups, ciberdelincuencia, información, preservación.

ABSTRACT

Information is one of the most necessary assets for the different entities that exist and not only for them but it is also important individually or personally, however, something that seems easy to manage has become complex due to the growing demand for information that day a day is accumulated without having the spaces required and then complicating their search, in addition, in the constant and rapid evolution of technology has been affected their permanence putting at risk of total loss, since many have not followed the due actions and whether for lack of knowledge, or that, due to technological advances, new versions emerge and the compatibility between formats and devices is nil, making it difficult to maintain this information, that is why it is necessary to publicize the different storage methods and give the best options to keep those documents of great importance for a user safe, which is achieved Updates and backups by means of reliable media and capable of maintaining and migrating information in the future.

Keywords: Files, backups, cybercrime, information, preservation.

INTRODUCCIÓN

La necesidad de conservar los datos generados a través del tiempo, mantener el soporte y que la seguridad de estos sea confiable, se ha convertido en tema de investigación para que los desarrolladores de software y de hardware cada día avancen, generando soluciones en cuanto a productos que logren abarcar la problemática de almacenamiento para que cuyos documentos perduren a largo plazo siendo esto, esencial para el éxito de la gran mayoría de negocios, ya que basado en ello, se pueden generar mejoras, debido a que por medio de esta información se pueden realizar análisis estadísticos, confiabilidad en los negocios con respecto a los clientes y así sucesivamente, para tomar las mejores decisiones y lograr el reconocimiento y el buen nombre.

Pero no solamente está la necesidad de almacenamiento y conservación sino que surge la necesidad de protección y aseguramiento de los datos generados y almacenados en las distintas entidades, debido a eso se hace necesario dar a conocer de las metodologías empleadas para lograrlo con la mayor pertinencia del caso, utilizando los medios tecnológicos, las técnicas adecuadas y así implementar las medidas de seguridad de la información, con el fin de evitar desastres que pueden ser ocasionados por diferentes factores que la ponen en riesgo; dichos riesgos pueden producirse ya sea por fallas humanas (con o sin intención), por desastres naturales o fenómenos ambientales entre muchas causas más que se presentan, razón por la cual es importante evaluar los niveles de riesgos e identificar las vulnerabilidades en los sistemas informáticos incluyendo la protección a la ciberdelincuencia.

2. PLANTEAMIENTO DEL PROBLEMA

Las tecnologías de información, en la actualidad, son la herramienta esencial para el procesamiento de los datos manejados en los diferentes tipos de organizaciones y en consecuencia, cada día se incrementan los volúmenes de información, haciendo más tediosa la tarea de conservarlos debido a la capacidad de almacenamiento de los medios como son el hardware y el software ya que a diferencia de los libros o formato papel que son mucho más elegibles para la búsqueda de un tema puntual debido a que está visualmente a la mano, los archivos digitales muchas veces no se sabe a simple vista qué documentos existen y cuál es su contenido si no se lleva de una manera organizada el almacenamiento; un ejemplo de esto es la situación que se presentó en el Archivo General de la Nación y que ha sido expuesta por investigadores como Olmo Uscátegui[1] en su investigación para su tesis de maestría en Antropología Social, consulta el Archivo Histórico del Magdalena Grande donde encuentra algunos ya destruidos y otros en muy mal estado a punto de perderse debido a las condiciones físicas en que se encontraban, dicha información era muy importante para la nación y el ministerio de cultura en Colombia. Otro investigador Hugo Buitrago[2], docente investigador de la Universidad Pontificia Bolivariana habla de la dificultad para acceder a información histórica en Sogamoso de vital importancia para el país en donde su estado higiénico y desorden en el que se encuentran.

Aunque es necesario conservar los medios físicos de los documentos (en papel), estos corren muchos riesgos de diferentes tipos, entre los cuales se encuentran amenazas por desastres naturales, como son las lluvias e inundaciones, terremotos, etc, o accidentes, como, por ejemplo; incendios producidos por cortos circuito o ya sea por acciones malintencionadas de personas; como evidencia de esto se encuentran muchos casos como el mencionado en el Blog especializado en Sistemas de Gestión de Seguridad de la Información[3] acerca del huracán Katrina y terremotos a través de la historia que han arrasado con empresas en diferentes lugares y solo aquellas que tienen un plan de contingencia y recuperación se han mantenido luego de tales sucesos.

---

[1] COPYRIGHT © 2020 PUBLICACIONES SEMANA S.A. Así se están muriendo algunos archivos en Colombia: PATRIMONIO | 7/9/2016 12:00:00 AM [en línea] [consultado 5 de 04 de 2020] disponible en: https://www.semana.com/cultura/articulo/documentos-en-riesgo-con-valiosa-informacion-historica/481149

[2] PUBLICACIONES SEMANA S.A. Ibíd., https://www.semana.com/cultura/articulo/documentos-en-riesgo-con-valiosa-informacion-historica/481149

[3] Blog especializado en Sistemas de Gestión de Seguridad de la Información [sitio web] Algunos ejemplos de incidentes de seguridad de la información16 febrero, 2017ISO 27001:2013. [consultado: 30 de abr. de 20]. Disponible en: https://www.pmg-ssi.com/2017/02/algunos-ejemplos-de-incidentes-de-seguridad-de-la-informacion/

A menudo se habla de seguridad informática y se utilizan métodos o técnicas de protección de datos, pero ante la gran necesidad de conservación de la información tanto personal como en las distintas empresas u organizaciones surge entonces la pregunta ¿De qué forma se puede crear copias digitales para preservar documentos y asegurar su disponibilidad a largo plazo?

3. JUSTIFICACIÓN

En la actualidad, muchas organizaciones aun no establecen medidas de control con el manejo de la información, ignorando que el aseguramiento y las políticas establecidas para controlar los riesgos es vital para su permanencia, ya que el peligro de desastres y pérdida de la información aumentan cada día y por causa de esto pueden desaparecer.

Además de ser importante, el respaldo de información para las distintas entidades particulares o tipo gubernamental, es de carácter obligatorio según las normas y decretos establecidos en la constitución colombiana como es Ley 1581 de 2012 en la que se establece el Régimen General de Protección de Datos en Colombia y el Decreto Reglamentario 1377 de 2013[4] para darles el debido tratamiento a los datos confidenciales obtenidos de los usuarios, ofreciendo así confiabilidad, confidencialidad e integridad en sus operaciones y generación de información; se pretende entonces con la presente investigación que las empresas y organizaciones comprendan la necesidad de llevar un control seguro y el más adecuado para proteger sus archivos y que obtengan la información precisa de cómo solucionar el problema en el almacenamiento y aseguramiento de sus documentos, de manera que conozcan tanto los riesgos a los cuales se exponen como también las medidas a tomar para evitarlos.

Mundialmente se han reconocido modelos y técnicas que se emplean para identificar factores de riesgos en los sistemas informáticos como por ejemplo COBIT, ISO 2701 de 2013, OCTAVE y muchas más que pueden ser implantadas según la necesidad y el tamaño de la entidad y según los requerimientos internos de ésta, por lo tanto, el presente trabajo monográfico brinda la información necesaria para aquellas entidades que desean contar con respaldos de copias de documentación digital a largo plazo.

[4] Ley Estatutaria 1581 de 2012 - Secretaría del Senado. [en línea] Diario Oficial No. 48.587 de 18 de octubre de 2012 CONGRESO DE LA REPÚBLICA. [consultado: el 19 de mayo de 2020] disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

4. OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar las diferentes formas en que se pueden crear copias digitales de documentación para asegurar la disponibilidad y la preservación a través del tiempo

3.2 OBJETIVOS ESPECÍFICOS

- Identificar las diferentes metodologías utilizadas para mantener copias de seguridad que ayuden a la preservación documental digital

- Establecer medidas de seguridad de la información mediante estrategias para la conservación documental digital

- Describir los procedimientos de la gestión de riesgos utilizando metodologías que ayuden a resguardar la información digital.

- Demostrar los beneficios de contar con el respaldo de la documentación digital

5. MARCO TEORICO

En los últimos años la tecnología ha crecido en gran manera en sus diferentes áreas y en especial, las telecomunicaciones y sistemas de manejo de la información, por lo cual, las organizaciones han tenido que enfrentarse a esos cambios ya que en sus procesos diarios se generan grandes cantidades de datos que solo con el apoyo de herramientas tecnológicas como lo es una computadora entre otros dispositivos, facilitan la tarea, reduciendo el tiempo empleado para realizar consultas de documentos aun sin importar la ubicación geográfica de las empresas y sus sedes ya que remotamente los archivos o documentos pueden ser manipulados por personas autorizadas.

Con este avance y sus procesos automatizados surge la necesidad de organizar y conservar la información utilizando los medios posibles y eficaces para ello.

Figura 1. Organización de la información

Fuente: Rojas, Elisabeth. [sitio web] La historia del almacenamiento y la recuperación de datos mcpro 27 marzo, 2014 [consultado: noviembre 13 de 2020] disponible en: https://www.muycomputerpro.com/2014/03/27/historia-almacenamiento-recuperacion-datos#:~:text=En%201932%2C%20las%20memorias%20de,logran%20almacenar%20datos%20en%20ADN.

A través de la historia, se pueden ver los primeros signos de escritura que surgen de la necesidad de guardar información como son los registrados en tablas de arcilla secados al sol y que con el tiempo fueron evolucionando dichos métodos, llegando a la época moderna con el uso del papel, sin embargo, a mediados del siglo XIX se reconoce el problema que atañe al método de uso del papel el cual fue llamado papel friable que según, es el alto grado de deterioro de dicho material.[5]

La necesidad de conservación y transmisión trae consigo múltiples formas de almacenar la información danto origen a las primeras copias digitales por medio de instrumentos como fue el tele-diágrafo utilizado en el año 1985 cuyo propósito fue el de transformar las imágenes a formato digital y enviarlas por métodos eléctricos.

Para 1913 se utilizó el belinógrafo, dichas transmisiones realizadas, fueron las conocidas como el FAX y aunque las computadoras surgieron para los años 40, no fue sino hasta los años 80 que se fabricaron los escáneres digitales por primera vez; donde ya era posible guardarlos o almacenar los archivos de tipo imagen permitiendo de esta manera a que la información de éstas se podía reproducir, consultar y hasta publicar en internet.[6]

Es entonces para 1977 que surgen los primeros indicios de la preservación documental a través de las redes, debido a las amenazas cibernéticas en donde el senador Abraham A. Ribicoff, EUA, propone un "Acta de Protección de los Sistemas de Cómputo Federales" lo que permite dar los primeros pasos hacia la seguridad informática.

La historia de la escritura como tal, va relacionada con la búsqueda de la automatización de esta misma, por medio de herramientas que faciliten el almacenamiento de la información; de esta manera surge la informática con inventos como fue la maquina automática de tarjetas perforadas creadas en 1884 por Herman Hollerithy; con fines de almacenamiento y procesos estadísticos dando origen más tarde a la cinta magnética como un medio de respaldo de la información[7]

---

[5] Technical Guidelines for Digitizing. [sitio web]. Cultural Heritage Materials Creation of Raster Image Files. Septiembre 2016. [consultado: el 19 de mayo de 2020] Disponible en: http://www.digitizationguidelines.gov/guidelines/FADGI%20Federal%20%20Agencies%20Digital%20Guidelines%20Initiative-2016%20Final_rev1.pdf

[6] Centro de Conversión de Documentos e Imágenes, S.A. de C.V.[Imaging Cente] [en línea]: Origen y concepto de Digitalizacion
El equipo de marketing Digitalizacion. [consultado: el 18 de abr. de 20] disponible en: http://www.imaging.mx/origen-y-concepto-de-digitalizacion/

[7] Historia de la informática. [sitio web]. Historia de las bases de datos. 4 de enero de 2011 [consultado: 13 noviembre 2020] disponible en: https://histinf.blogs.upv.es/2011/01/04/historia-de-las-bases-de-datos/

Figura 2. Discos magnéticos

Fuente: Historia de la informática. [sitio web] Historia de las bases de datos. 4 de enero de 2011 [consultado: 13 noviembre 2020] disponible en: https://histinf.blogs.upv.es/2011/01/04/historia-de-las-bases-de-datos/

Para continuar, es importante aclarar que no es lo mismo la seguridad Informática y la preservación documental digital ya que la seguridad Informática se encarga de las diferentes estrategias para la protección de la información aplicando métodos y estableciendo políticas que se encarguen de evitar daños o deterioros o cualquier situación que le ponga en peligro. En cuanto a la preservación documental es el soporte y la forma de cómo se conservará ésta, siendo importante los medios utilizados para que la información perdure y sea compatible con los soportes tecnológicos sin importar el paso del tiempo.

En la investigación publicada por la revista digital ***scielo*** en el artículo “Investigación bibliotecológica” establece dichas diferencias como se muestra a continuación:
En el caso de preservación documental digital debe establecerse específicamente cómo esos documentos serán conservados durante y a través de las diferentes generaciones de la tecnología a través del tiempo, con independencia de donde residan —sus soportes— y de cómo estén representados —sus formatos—.”

También define "Seguridad Informática" como:

“*El proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización y que administren el riesgo al garantizar en la mayor medida posible el correcto funcionamiento ininterrumpido de esos recursos”.*[8]

[8] Investigación bibliotecológica

Una vez definidos ambos términos es importante mirar las leyes y estándares que rigen para ambos.

La seguridad Informática abarca una serie de normas y procedimientos con las cuales las entidades se ven en la obligación de adoptar con el fin de que garantizar la protección de la información y aún más la que tiene que ver con datos sensibles que garanticen la confidencialidad e integridad de dichos datos como son los estándares para la seguridad de la información emitidos por la "*Organización Internacional de Estándares (ISO) como ejemplo: el estándar ISO/17799 o los estándares ISO/IEC 27001 y 27002 (Information technology – Security techniques – Information security management systems – Requirements*)"; además, el estado también se ha encargado de crear normas y leyes para la llamada ciberdelincuencia de manera que, quienes infrinjan estas leyes son obligados a pagar ya sea multa salarial o con cárcel; esto, dependiendo la gravedad del asunto y pueden ser constatadas en el código penal de Colombia en donde aparecen en sus dos capítulos más recientes en la ley 1273 de 2009 en pronunciación a la protección de la información y de datos[9]

No obstante, el tema de la preservación documental digital también es respaldado por Acuerdo No. 006 de 15 OCT 2014 donde dice en una de sus partes que la Ley 594 de 2000 en el titulo XI "Conservación de Documentos", Artículo 46 establece: "Conservación de documentos. Los archivos de la Administración Pública deberán implementar un sistema integrado de conservación en cada una de las fases del ciclo vital de los documentos"[10].

Visto de esta manera es válido decir que establecer estrategias de preservación de documentos, es un compromiso con el que las organizaciones están obligadas a cumplir y el beneficio como tal es para sí mismas tanto, como los es para los usuarios en particular.

Cabe recordar que mediante los distintos avances tecnológicos que tienen que ver con el almacenamiento y procesos de la información siempre se ha buscado mantener la seguridad y protección de los datos y que la preservación de los documentos digitales es una de las formas más usadas en la actualidad.

[versión On-line] ISSN 2448-8321versión impresa ISSN 0187-358X
Investig. bibl vol.24 no.50 México ene./abr. 2010: Artículos Preservación documental digital y seguridad informática [consultado: 19 de abr. de 20] disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008#nota

[9] Seguridad de la Informacion en Colombia.[en línea]. martes, febrero 23, 2010. Marco legal de Seguridad de la Información en Colombia [consultado 19 de abr. de 20] disponible en: http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html

[10] Archivo General de la Nación Colombia. [en línea]. ACUERDO 006 DE 2014. 15 abril, 2014. [consultado 19 de abr. de 20] disponible en: https://normativa.archivogeneral.gov.co/acuerdo-006-de-2014/

6. MARCO CONCEPTUAL

Preservación

Según la Real Academia Española ([RAE],2020) es "Proteger, resguardar anticipadamente a alguien o algo, de algún daño o peligro"[11]

Documentos

El Concejo Internacional de archivos (ICA) afirma que "Los documentos de archivo son el subproducto documental de las actividades que desarrolla el hombre y son conservados a largo plazo por su valor testimonial."[12]

Por otra parte, una definición más a fin al presente trabajo se encuentra en DeConceptos.com donde dice que "Un documento es una información escrita, o voces, o ruidos grabados, o imágenes, en soportes varios, como papel, discos magnéticos, vidrio, mármol, etcétera, que pueden consistir en películas, títulos profesionales, grabaciones, marcas y señales, etcétera." [13]

Digital

Según lo encontrado en definiciones en la web, es aquello relativo a las huellas del ser humano y se relaciona en la actualidad a la tecnología y la informática para hacer referencia a la representación de información de modo binario encendido o apagado. [14]

Formato

El formato es el conjunto de las características técnicas y de presentación de un texto, objeto o documento en distintos ámbitos, tanto reales como virtuales. [15]

Existen diferentes aspectos que involucran el respaldo de documentos o archivos con los que se procede a realizar un almacenamiento con el fin de preservarlos, como por ejemplo los de tipo texto o de imágenes; así mismo existen diferentes medios de almacenamiento como son los medios físicos.

---

[11] © Real Academia Española, 2020.[en linea] [Consultado:30 de abr. de 20]. disponible en: https://dle.rae.es/preservar

[12] © International Council on Archives 2016.[sitio web]. [Consultado: 30 de abr. De 20] Disponible en: https://www.ica.org/es/%C2%BFqu%C3%A9-son-los-archivos

[13] De Conceptos.com Copyright © 2020. [sitio web] [Consultado: 27 de abr. De 20] Disponible en: https://deconceptos.com/ciencias-juridicas/documento

[14] Copyright © 2008-2020 - Definicion.de. [consultado: 27 de abr, de 20]disponible en: https://definicion.de/digital/

[15] Consultado en : https://www.google.com/search?q=formato&oq=formato&aqs=chrome..69i57j35i39l2j0l5.3764j0j7&sourceid=chrome&ie=UTF-8

Preservación Documental Digital

Figura 3. Sistemas de Gestión Documental

Qué es un sistema de Gestión Documental y cuáles son sus ventajas.
3 diciembre, 20192011 [consultado: 16 noviembre 2020] disponible en: https://www.imagine-cs.com/category/gestion-documental/

Según la terminología descrita anteriormente se deduce que la preservación documental digital es mantener a salvo la información en un documento y que ésta esté disponible a largo plazo y que a su vez cumpla con la confiabilidad de que no sea alterada ni modificada por terceros sino por quienes estén autorizados garantizando su autenticidad y accesibilidad; Ana Canteli[16] menciona en su boletín de noticias la importancia de la preservación de los documentos precisamente para conservar y mantener los pilares de la información considerando las dificultades que se enfrentan cada vez por el rápido avance de tecnologías en los que se ven afectados muchas veces por la dependencia de éstos al hardware y el software para su respectivo acceso, lo cual conlleva a la búsqueda de soluciones identificando cada paso para el proceso que deben llevar las organizaciones con el fin de implementar esta actividad de conservación de su información digitalmente para lograr un mejor desempeño en sus operaciones.

De esta manera, basados en la definición encontrada en el portal de la biblioteca de Catalunya[17] preservación digital también se puede definir como un conjunto de

[16] Open Document Management System S.L. [sitio web]. [consultado:5 de abr. De 20] disponible en: https://www.openkm.com/es/blog/conservacion-de-documentos-electronicos.html

[17] 2020 Biblioteca de Catalunya. [sitio web] Carrer de l'Hospital, 56. 08001 Barcelona. [consultado:5 de abr. De 20] disponible en: https://www.bnc.cat/esl/Profesionales/Preservacion-digital2

técnicas que se aplican metodológicamente para lograr la futura disponibilidad de la información en cualquiera de los campos que se necesite, es decir, esto se puede dar para formas culturales e históricas de una región como por ejemplo, las bibliotecas que para este caso tendrían que digitar aquellos documentos históricos para evitar su extinción o entidades de diferente índole pero con la misma necesidad de proteger la información y que en esta búsqueda se logre conservar a largo plazo con la opción de fácil recuperación y según información encontrada en la Revista Scientific[18] se define la preservación digital como la práctica de salvaguardar los recursos digitales que se necesitarán en un futuro siendo esto diferente a realizar copias de seguridad de las que se crean respaldos a diario y hasta en tiempo real y también se encuentra la definición de las *copias de preservación*, que, por el contrario, el método suele ser la actualización en los medios de almacenamiento de manera integral del todo el material, haciendo copiado del mismo periódicamente.

Otro concepto es el que se encuentra en la Revista Española de Documentación Científica dice de la preservación digital:

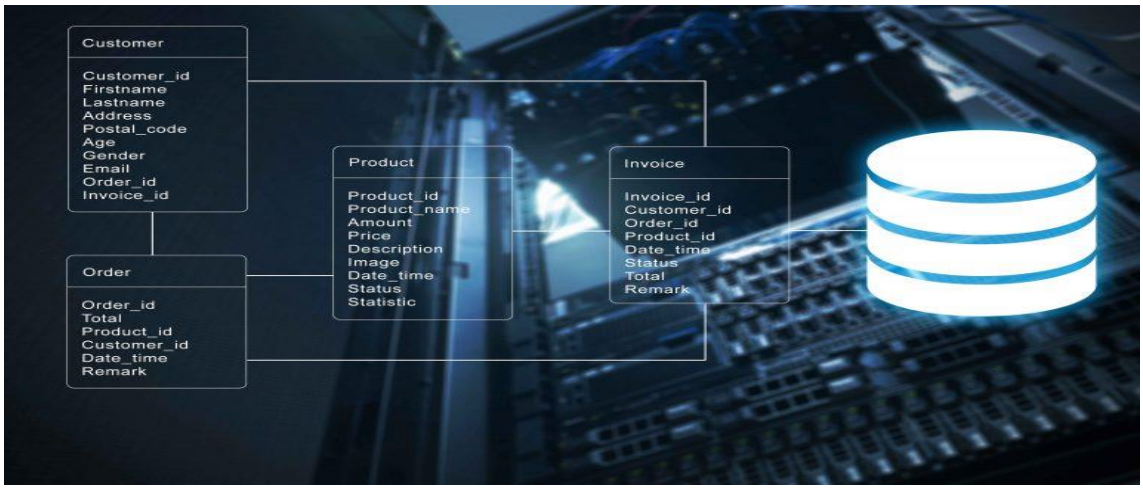
Que las barreras de índole organizativa, económica o legal pueden ser aún mayores que las técnicas. Por ello, en el libro se produce el relato sintético de los aspectos organizativos, financieros, legales y normalizadores que vienen a converger en una estrategia de preservación digital que pretenda ser sólida. Tras establecer los conceptos preliminares el manual hace hincapié en el célebre modelo OAIS (desarrollado inicialmente por la NASA y actualmente norma ISO); así como en las técnicas más evidentes: la actualización de soportes, la migración de formatos, la emulación, y el análisis forense digital.[19]

Base de datos

Figura 4. Bases de Datos

[18] Instituto internacional de investigación y desarrollo tecnológico educativo INDTEC. Revista scientific volumen 4, num.14 Revista Arbitrada Multidisciplinaria de Investigación Socio Educativa Volumen 4, N.º 14/ Noviembre-Enero2019-2020/ Venezuela/ Edición Trimestral [consultado 5 de abr. de 2020] disponible en: http://www.indteca.com/ojs/index.php/Revista_Scientific/issue/view/28/Scientific.issn.2542-2987.2019.4.14

[19] Miquel Térmens Barcelona: Editorial UOC, 2013 (El profesional de la información:16). 109 pp. ISBN 978-84-9029-819-0.



Fuente: Aplicaciones Informáticas de Bases de Datos Relacionales, Fundación Maude
C/ Donoso Cortés 9-11, 29002. [Consultado:[16 de noviembre de 2020] disponible en: https://www.fundacionmaude.com/wp-content/uploads/2017/08/bases_datos-768x510.jpg

Es un conjunto de información almacenada por medio de procesos lógicos y automatizados, con el fin de ser recuperada, consultada, analizada o transmitida a partir de la necesidad del ser humano, de preservar la información a largo plazo, pudiendo lograrlo con el apoyo de las tecnologías informáticas que ofrecen el fácil manejo de datos en sus diferentes procesos en las distintas entidades.

En la necesidad de almacenar y procesar los datos, contando con la tecnología, se han desarrollado bases de datos en diferentes modelos de implementación pero que al final ofrecen al usuario, conservar de la mejor manera grandes volúmenes de información según genere la organización.[20]

[20] "Base de datos". [en linea] . María Estela Raffino. De: Argentina. Para: Concepto.de. [consultado:5 de abr. De 20] Disponible en: https://concepto.de/base-de-datos/. [Consultado: 21 de abril de 2020]. Fuente: https://concepto.de/base-de-datos/#ixzz6KFsIhFDw

7. METODOLOGÍAS UTILIZADAS PARA MANTENER COPIAS DE SEGURIDAD QUE AYUDEN A LA PRESERVACIÓN DOCUMENTAL DIGITAL

Al aplicar un proceso para llevar a cabo la conservación documental se debe seguir una metodología de transformación manual desde un formato tipo papel a uno copiado técnicamente, por medio de las tecnologías con procesadores de información como, por ejemplo, una computadora con programas especiales para ello, como puede ser Word o en cualquier otro formato como son las imágenes. El proceso que se debe seguir es, pasar un formato papel a digital, cuya conversión es factible, tanto copiada textualmente o escaneada.
Como se mencionó antes, entre las entidades que más se han interesado en la copia de seguridad de documentos, están las bibliotecas que en su búsqueda de consérvalos, han construido patrimonios digitales como es el caso de UNESDOC Biblioteca Digital , pero cabe recordar que, en el mundo de los negocios, tener la información al alcance de manera rápida se hace cada vez más necesaria, exigiendo así la innovación tecnológica que a su vez tiene como objetivo satisfacer las necesidades, tanto en el sector científico como el comercial y financiero, teniendo esta vez en cuenta que la seguridad de la información requiere eficiencia y confiabilidad en los medios tecnológicos por lo que esta debe renovarse sin perder de vista la migración de los datos que van quedando en los medios de versiones anteriores y que a medida que surjan nuevas metodologías de almacenamiento y procesamiento van perdiendo la compatibilidad de lo cual nace la necesidad de hacer actualizaciones y mantenimiento en dichos medios en los cuales la documentación es procesada.

Vemos entonces un concepto de innovación que según *J.A. Schumpeter*, se trata de la “introducción de nuevos productos, servicios, procesos y fuentes de abastecimiento, como también cambios en la organización industrial, de manera continua y orientados al cliente, consumidor o usuario”.

7.1 SEGURIDAD DE LA INFORMACION

Todo lo que tiene que ver con el resguardo de los datos almacenados en un medio hardware y software, de manera que nada pueda interferir en su integridad lo cual hace que dicha información sea confiable. Al brindar una forma de protección, se hace mención a la **seguridad de la información** la cual reúne muchas técnicas y medidas para poder controlar todos los datos generados ya sea en organizaciones donde se hace necesario crear copias de seguridad de todos los procesos que se llevan a diario, **copias de preservación** de información importante la cual se debe mantener actualizada debido a las nuevas tecnologías con las que se pierde la compatibilidad de formatos en los diferentes medios de almacenamiento.

En la seguridad de la información existen tres aspectos principales que se deben mantener siempre que son la confidencialidad, disponibilidad y la integridad términos definidos por ©2019OBS de la siguiente manera:

Confidencialidad, garantiza que los datos que están guardados en el sistema no se divulguen a terceros no autorizados.

Disponibilidad, la información guardada en el sistema, tiene que estar siempre a disposición de los usuarios autorizados en cualquier momento.

Integridad, garantiza que los datos no deben manipularse o modificarse a no ser con autorización por orden expresa. [21]

La seguridad de la información es muy importante cada vez más ya que surge la necesidad en diferentes sectores como son [22]"los Gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas acumulan una gran cantidad de información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera. La mayor parte de esta información es recolectada, tratada, almacenada y puesta a la disposición de sus usuarios, en computadoras y trasmitida a través de las redes entre los ordenadores." Según lo expone ©2019-Unilibre.
A partir de la anterior contextualización se puede afirmar que es un requisito de orden legal para las diferentes entidades u organizaciones mantener la Seguridad de la Información, lo cual exige la incorporación de nuevas áreas en el conocimiento especializado para la implementación de la protección de datos dentro de las empresas las cuales se mencionan a continuación como ejemplo y más comunes los **sistemas de gestión de riesgos**, que se llevan a cabo a través de procedimientos técnicos utilizando metodologías y códigos de buenas prácticas con el fin de velar por todo el sistema implementado en estas, otra área de conocimiento son **las auditorías** certificadas por normas y estándares que rigen y regulan para que se hagan con total transparencia y confiabilidad de parte de las personas o profesionales en este campo, las auditoría de sistemas de información, permiten checar que todo esté en orden y a la vez actualizar sistemas de protección para controlar y minimizar riesgos.

[21] Planeta Formación y Universidades Instituciones educativas OBS Business School.[en linea] [consultado:5 de abr. De 20] disponible en: https://www.planetaformacion.com/es/instituciones-educativas/obs-business-school

[22] Copyright © 2019 Unilibre Institución de Educación Superior sujeta a inspección y vigilancia por el Ministerio de Educación Nacional. Personería jurídica Res. 192 de 1946-06-27 – Ministerio de Gobierno. [consultado: 7 de abr. De 20] disponible en: https://www.mintrabajo.gov.co/documents/20147/58606751/VALLE+DEL+CAUCA+AFL+UNIVERSIDAD+LIBRE+SUSCRITO.pdf

7.2 CREACION DE COPIAS DIGITALES

Para crear copias digitales es necesario saber de medios de almacenamiento, sus diferentes clases y versiones con los que se hará el respaldo de los documentos a proteger, pero no sin antes mirar la historia de los primeros medios utilizados para la realización de esta tarea como se muestra a continuación.

7.2.1 MEDIOS DE ALMACENAMIENTO DE INFORMACIÓN MANUALMENTE

7.2.2 PAPEL

Figura 5. Papel

FUENTE: PAPEL. [Consultado: 16 de noviembre de 2020] disponible en : https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcQdAQS8ZEK8rH46RggO7j700FpP2sgDR3Spf-jfAOLhQiOnDNoT

La historia cuenta que fue inventado por Ts'ai Lun, en el año 105 d. C. Se dice que este empezó creando láminas de papel utilizando telas, cortezas de árboles y redes de pescar.
Un pequeño pueblo de la región de Las Marcas, que en el siglo XII empezó a fabricar papel utilizando lino y cáñamo, hizo estudios de nuevos equipos y técnicas de producción, introduciendo importantes innovaciones:

- Mecanizaron la moledura de las hilachas
- El encolado de las hojas con gelatina animal
- Crearon varias clases de papel
- Inventaron el afiligranado de las hojas

7.2.3 LIBROS

Figura 6. Libros

Libros. Gerhard Gellinger. [sitio web] Nürnberg/Deutschland. [Consultado: 7 de abr. De 20] Disponible en: https://pixabay.com/es/photos/lib

La historia del libro se remonta al año 4000 a.C cuando los sumerios de Mesopotamia meridional de quienes se encuentra el primer sistema de escritura documentado llamado escritura cuneiforme.

Este sistema de escritura empleaba **tablas de arcilla** y símbolos hechos con objetos puntiagudos. Para 2400 a.C se encuentran los rollos de papiro inventados en Egipto, producidos de una planta que crece a orillas del rio Nilo y que luego de procesarla servía para escribir con un cálamo afilado.

Al llegar al siglo II, a.C se descubre un nuevo material de escritura llamado pergamino, hecho de material más resistente, por lo tanto, de mejor calidad que los mencionados anteriormente. Otros inventos fueron la tablilla de cera descubiertas

en roma, estas fueron precursoras del término encuadernación dando paso a los primeros libros llamados códices y que a la vez fueron de las mayores innovaciones en Roma en ese siglo.

La gran revolución reside en la comodidad del formato, más cómodos por su contextura, tamaño y facilidad de leer.

Sin embargo, los paganos y el pueblo judío amaban sus tradicionales métodos de escritura y lectura. Por otra parte, estaba la comunidad cristiana que acogió con entusiasmo la novedad descubierta, con los monjes que transcribían en los códices oraciones y textos sagrados.

7.2.4 MANUSCRITOS ILUMINADOS

Figura 7. *Manuscritos Iluminados*

Fuente: Manuscritos iluminados. Imagen de Hans Braxmeier. [Consultado: 7 de abr. De 20]. Disponible en: Pixabay.com

Si bien el papel ya se había inventado desde el año 105 d. C no se hizo el primer libro encuadernado con páginas en este material y otros los mencionados hasta el 400-600 d. C. cuando aparecieron los primeros manuscritos iluminados en hojas de pergamino**.**

Definidas las anteriores formas en los inicios de la escritura ahora se puede hablar de almacenamientos en la informática.

7.3 DISPOSITIVOS DE ALMACENAMIENTO DIGITAL

Desde tiempos antiguos el hombre ha sentido la necesidad de superar sus limitaciones por lo que ha acudido a diferentes tipos de herramientas según la necesidad que afronte en su diario vivir con el fin de hacer más fácil aquello que le resulte tedioso o complicado.

En el caso del manejo de la información y centrándose en la parte de realizar cálculos el ser humano buscó inicialmente la solución brotando como resultado según la historia el **ábaco,** esta fue una herramienta inventada por los babilonios por los años 3.000 a.C y así sucesivamente fueron apareciendo nuevos inventos que realizaban cada vez operaciones aún más complejas como fue la pascalina, la maquina diferencial, la maquina tabuladora, etc; solo hasta 1939 aparece el primer computador electrónico basado en relés, construido por Howar Aiken llamando al dispositivo MARK1 el cual fue remplazado por el ENIAC siendo este el primer computador digital electrónico.

A través de la historia se establecen las invenciones digitales por épocas en las que surgen mejoras y nuevas versiones dejando atrás el gran tamaño de los dispositivos y con el descubrimiento del transistor se logra mayor eficiencia en software y movilidad en el hardware, estos espacios de tiempo van desde primera hasta la sexta generación conociéndose así la tecnología que hoy día se emplea para el almacenamiento de diferentes tipos de datos en diferentes programas o aplicaciones dependiendo el uso y la necesidad del procesamiento de la información.[23]

Los fabricantes tecnológicos han creado muchos medios de almacenamiento que soportan gran cantidad de archivos en diferentes formatos multimedia o texto en sus muchas variedades de extensiones existentes. Ejemplo: imágenes gif, jpg, tex, pdf, etc.

[23] Castro Carmona, Ariel. Arquitectura de computadores. Bogotá, D.C, 1995

7.3.1 CINTA MAGNÉTICA.

Ilustración 2. Cintas Magnéticas

Fuente: pixabay.com. Cinta magnética. [consultada el 4 de abril de 2021] disponible en: https://pixabay.com/es/photos/cinta-magn%C3%A9tica-reel-to-reel-vintage-401189/

Fue de los primeros inventos de tipo de almacenamiento extraíble, conocidas como cintas perforadas.

7.3.2 DISCOS MAGNÉTICOS RÍGIDOS

Aquí se incluyen los medios de almacenamiento como son la CPU, Tarjeta madre y las memorias RAM, dando paso a los discos duros y así mismo a los computadores personales.[24]

Figura 8. Disco Magnético Rígido

[24] Ciriaco García de Celis (1994). «El disco duro del AT (IDE, MFM, BUS LOCAL).». (4ª edición). Facultad de Ciencias de Valladolid: Grupo Universitario de Informática

Fuente: Figure discos magnéticos. Imagen de OpenClipart-Vectors. [Consultado:16 de noviembre de 2020] disponible en: Pixabay.com

7.3.3 DISCO DURO.

Tienen la capacidad de almacenar gran cantidad de información y pasarla de un dispositivo a otro

7.3.4 CD.

Los CD almacenan menor cantidad de información que los discos duros pero tienen la capacidad de portar información desde un dispositivo a los destinatarios de correcta autenticación

7.3.5 LAS MEMORIAS USB.

También almacenan copias de seguridad conectándose en los discos duros y migran información de los documentos almacenados protegiéndolos del hurto de su contenido.

7.4 BACKUPS.

Figura 9. Gestión de Seguridad

Fuente: Figure backups. [en linea] Guía práctica para realizar backups. jjvelasco - Abr 8, 2011 - 19:34 (CET). [consultado: 20 de Mar. 5 de 20] Disponible en: https://hipertextual.com/archivo/2011/04/guia-practica-backups/

Tienen la capacidad de respaldar las copias desde una computadora a través de los medios tecnológicos usados para tal fin, de manera que giren en el entorno de donde se abrirán nuevamente.

8 AMENAZAS, ATAQUES Y MEDIDAS DE SEGURIDAD INFORMATICA MEDIANTE ESTRATEGIAS PARA LA CONSERVACIÓN DOCUMENTAL DIGITAL

8.1 AMENAZAS Y VULNERABILIDADES DE ACTIVOS DE INFORMACION

Las posibles amenazas que pudieran surgir en el escenario planteado como son los procedimientos de almacenamiento de información en los diferentes medios y formatos ya expuestos, se pueden presentar con la ocurrencia de incidentes que llevan a la pérdida total o parcial de datos.
Entre las amenazas a sistemas informáticos se encuentran las siguientes[25]

8.1.1 LÓGICAS

Son causadas por errores por defecto de programación en los diferentes sistemas operativos, como ejemplo se tienen los gusanos o virus que aprovechan los bugs para expandirse.

8.1.2 DE USUARIOS

Los mismos usuarios pueden ser una amenaza para los sistemas informáticos, ya que por error o desconocimiento pueden dañar o borrar archivos; de otra forma también puede ser intencional por lo que se debe tener personal de confianza y ser responsable de las autorizaciones y contraseñas de usuarios para el acceso al sistema.

8.1.3 AMENAZAS FISICAS

Entre estas amenazas se encuentran las que son causadas por desastres naturales, robo o sabotaje y de tipo eléctrico.
A continuación, se mencionan las más significativas.[26]

[25] Configuración de Mecanismos de Seguridad. Tipos de amenazas físicas U8. [sitio web] [consultado 2 de may. de 20]. https://virtual.itca.edu.sv/Mediadores/cms/u48_tipos_de_amenazas_fsicas.html

[26] Prakmatic 2017. [sitio web]. Principales amenazas de un sistema informático. [consultado 2 de may. de 20]. Disponible en: http://www.prakmatic.com/uncategorized/principales-amenazas-de-un-sistema-informatico/

8.1.4 FUGA DE INFORMACIÓN

Se puede presentar por parte del personal que labora en las empresas, en donde por represalias algunos integrantes pueden valerse de sus conocimientos para infiltrarse en los sistemas y exponer información importante y vital para su funcionamiento.

8.1.5 DAÑO EN DOCUMENTOS Y DATOS SENSIBLES

En materia documental, se puede sufrir perdida y daño de información importante como Facturas, Proyectos, Hojas de vida del personal de planta, Formularios de seguimiento, Proyectos, Planos, entre otros acervos documentales de gran importancia para las organizaciones o entidades.

8.1.6 DAÑO A LA INFRAESTRUCTURA DE LOS SISTEMAS DE INFORMACIÓN

Una de las causas de esta amenaza se puede ocasionar por la fuga de información donde se develarían cuentas administradoras y claves de acceso, con las cuales se atacaría la infraestructura de los sistemas de información de cualquier entidad, causando daño a datos, extracción de información esencial e indisponibilidad de los sistemas de información con el fin de dañar la imagen de la institución.

8.1.7 DAÑO A ELEMENTOS TECNOLÓGICOS Y SOPORTES

Este tipo de amenaza puede ocurrir en caso de la inundación, donde pueden quedar comprometidos los equipos de la infraestructura tecnológica, así como daños a elementos electrónicos como son memorias, discos y soportes en papel, etc.

8.1.8 PÉRDIDA DE INFORMACIÓN Y DAÑO DE DOCUMENTOS

Esta amenaza se puede presentar por mala ubicación de archivos y expedientes de las entidades exponiéndose ante una posible pérdida del acervo documental y expedientes esenciales para el funcionamiento a causa de inundaciones por el desbordamiento de ríos o el fenómeno de fuertes lluvias, entre otros.

8.1.9 RIESGO ELÉCTRICO

Esta amenaza pude exponer la integridad y seguridad de la información y puede ser causada por cortos circuitos o accidentes por falta de mantenimiento en las redes

eléctricas de las organizaciones pudiendo ser esto la principal causa de los incendios. [27]

8.1.10 TERREMOTOS

Este fenómeno natural puede ser causante de:

Daño en infraestructuras

Esta amenaza puede causar pérdida material de equipos ofimáticos, bases de datos y documentación esencial que soporte el contenido de archivos o documentos.

Pérdida de información

Es una amenaza que se debe enfrentar después de un terremoto, ya que, debido al colapso y caída de la infraestructura de la entidad, se producen daños a equipos de cómputo, servidores, data center y archivos o acervos documentales esenciales para el funcionamiento de la organización que, en la mayoría de los casos, quedan irrecuperables.

Indisponibilidad de los sistemas de información

Esta amenaza causada por el daño a los servidores y bases de datos y demás elementos que se vieron afectados por terremotos, inundaciones o cualquier otra causa de riesgos es muy importante ya que ocasiona pérdidas irrecuperables si no se tienen las medidas de seguridad correspondientes.

[27] Seguridad informática [sitio web]. Jhonsar 2010. [consultado: 2 de may. de 20] disponible en: https://www.blogger.com/profile/11714127096787219444

8.2 ATAQUES

La seguridad de la información es muy importante para estar confiados de tener óptimos procesos y un buen desempeño en las empresas por lo que se requiere invertir tiempo en la gestión de esta.

Aunque el peligro en el que se encuentra la información se presenta desde un lugar físico, así como en el proceso y transmisión de esta generalmente la información es almacenada en bases de datos por lo cual se describirá a continuación:

Los diferentes ataques que se presentan sobre ellas y las vulnerabilidades que pueden tener estas para que den dichos ataques poniendo en riesgo la disponibilidad de la información en cualquier entidad y especialmente a la que se encuentra en la nube; por eso es muy importante concientizarse de que cada vez se levantan nuevas vulnerabilidades debido al crecimiento o surgimiento de nuevas tecnologías y para esto se debe estar prevenidos por medio de los controles necesarios que permitan una excelente seguridad en los sistemas de información y formar una berrera muy fuerte ante los ataques en servidores y demás hardware de uso de almacenamiento de datos.

Por medio de diferentes metodologías que establecen secuencias normativas se puede lograr establecer medidas que previenen que un ataque tenga éxito, por eso es necesario realizar auditorías periódicamente que conlleven a establecer si han surgido nuevas vulnerabilidades las cuales tienen que ver con los **Aspectos éticos y legales** que abarcan el tema de la seguridad informática, fundamentados en conocer los valores y deberes éticos, las responsabilidades profesionales, los imperativos y preceptos morales. Estos aspectos se parametrizan a través de las leyes internacionales y locales para regir el comportamiento humano en contra de los delitos informáticos.

8.2.1 ATAQUES A LOS SISTEMAS DE BASE DE DATOS

Para entender de los ataques a los sistemas de bases de datos se debe saber primero que es una base de datos por lo que se explicará en detalle a continuación.

8.2.2 CARACTERÍSTICAS DE LAS BASES DE DATOS

Una base de datos se caracteriza por su variabilidad en la forma de sus procesos que bien pueden ser estáticos o dinámicos y por su contenido que puede ser

bibliográfico, de texto como es la documentación histórica y a la vez fuente primaria, directorios o contenido especializado.

“Aparte de sus características existen dos tipos de bases de datos que son las relacionales; en estas bases de datos o se hace la operación entera o no se hace utilizando la famosa técnica del rollback, los datos deben cumplir requisitos de integridad tanto en tipo de dato como en compatibilidad y están las no relacionales o NoSQL, que poseen escalabilidad y carácter descentralizado, aportan estructuras distribuidas, suelen ser bases de datos mucho más abiertas y flexibles, permiten adaptarse a necesidades de proyectos mucho más fácilmente que los modelos de Entidad Relación, además se pueden hacer cambios de los esquemas sin tener que parar bases de datos, escalabilidad horizontal, es decir, son capaces de crecer en número de máquinas, en lugar de tener que residir en grandes máquinas.”[28]

Las bases de datos también se identifican según la marca comercial y las principales que se mueven en el mercado son las siguientes:

DB2
SQL Server
Oracle
IBM
Teradata

Bases de datos no relaciones:

MongoDB
DynamoDB
Cassandra
Couchbase

Bases de datos relacionales:

Microsoft SQL Server.
Oracle.
DB2.
PostgreSQL.
MariaDB
MySQL. [29]

[28] NoSQL vs SQL. [en linea]. principales diferencias y cuándo elegir cada una de ellas noviembre 18, 2015 [consultado 21 de abr. de 20]disponible en: https://blog.pandorafms.org/es/nosql-vs-sql-diferencias-y-cuando-elegir-cada-una/

[29] Tipos de bases de datos y las mejores bases de datos del 2016. [sitio web]. blog.pandorafms.org: noviembre 18, 2015. https://blog.pandorafms.org/es/tipos-de-bases-de-datos-y-las-mejores-bases-de-datos-del-2016/

Hasta el momento se han descrito un poco sobre las bases de datos y conociendo la naturaleza de estas queda claro que queda de parte del cliente cual escoge según los requerimientos de su organización y el objetivo principal de estas es mantener o conservar los datos según su formato para posteriores consultas y lo ideal contar con dicha información cuanta vez se necesite.

No obstante, muchas veces se ignora la parte de la seguridad de las bases de datos ya que se adquieren, se instalan y no se prevé un procedimiento que asegure la adecuada configuración en la en su implementación con el fin de evitar lamentables perdidas.

Son muchas las causas de que esto pueda ocurrir ya que la información puede estar en riesgo debido a muchas amenazas, que suelen ser por accidentes por falla humana, por fenómenos de la naturaleza o por delincuentes cibernéticos.

8.2.3 VULNERABILIDADES DE LAS BASES DE DATOS

Según, un informe de Verizon (Data Breach) revela un alto porcentaje en ataques a bases de datos en más de 90%. [30]

Los ataques también mencionados en Ona sistema que son 10 de las más comunes como se muestra en la figura 10

[30] TICbeat: Tecnología Las 10 grandes amenazas de seguridad en las bases de datos. [en linea] Axel Springer : 17 April, 2013 España. [consultado 21 de Abr.de 20]

Figura 10. Las 10 Vulnerabilidades más comunes

Fuente: Ona Systems. [en linea]. Vulnerabilidades importantes que afectan la seguridad de bases de datos en las empresas [consultado 21 de abr. de 20] disponible en: https://www.onasystems.net/wp-content/uploads/2016/09/Bases-de-datos-Vulnerabilidad.jpg

Vulnerabilidades en BD.[31]

- Privilegios excesivos
- Abuso de privilegios
- Elevación de privilegios no autorizados
- Vulnerabilidades de la plataforma
- Inyección de sql
- Auditoría débil

31

- Denegación de servicio
- Vulnerabilidades en los protocolos de las bases de datos
- Autenticación débil
- La exposición de los datos de backup. [32]

Como se puede observar, estas son solo unas de las muchas vulnerabilidades que tienen las bases de datos y por las cuales son propensas a ataques de diferentes tipos.

9 ATAQUES POR INYECCION DE CODIGO

Figura 11. *Inyección SQL*

Fuente: Inyección SQL[sitio web]. Una guía para usuarios principiantes de WordPress Shaumik Daityari: febrero 6, 2020[consultado el 16 de noviembre de 2020] disponible en: https://kinsta.com/es/blog/inyeccion-sql/

Consiste en modificar el comportamiento de las consultas a través de introducción de parámetros no válidos, en los campos de acceso del usuario.

"Un ataque de este tipo puede dar acceso a alguien a una base de datos completa sin ningún tipo de restricción, pudiendo llegar incluso a copiar y modificar los datos."[33]

[32] © Copyright 2018 Ona Systems. [en linea]. Vulnerabilidades importantes que afectan la seguridad de bases de datos en las empresas [consultado 21 de abr. de 20] disponible en: https://www.onasystems.net/wp-content/uploads/2016/09/Bases-de-datos-Vulnerabilidad.

[33] AcensTechnologies. [sitio web]. Bases de datos y sus vulnerabilidades más comunes. [consultado 21 de abr. de 20].Disponible en: https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf

Es también una técnica utilizada por delincuentes o malintencionados que escriben instrucciones de Transact-SQL que no son entradas válidas. Las consecuencias de que un código de estos se ejecute resultaría en grades pérdidas para la organización. Las vulnerabilidades a los ataques de este tipo se dan debido a errores de validación de variables como, por ejemplo:

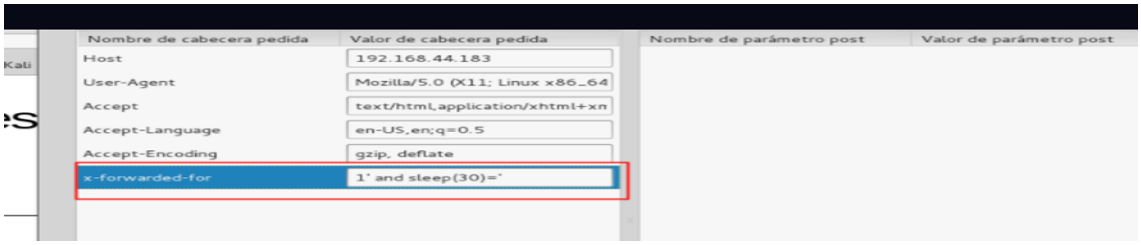
Los métodos que se emplean para atacar luego de encontrar el punto crítico son los siguientes:

Boolean-Based Blind

La inyección SQL ciega basada en expresiones Boleanas (verdadero o falso) que identifica los sitios web con los que se puede utilizar este método como se observa a continuación www.sitioweb.com/index.php?id=3 AND 1=0 // falso o, puede arrojar 1=1 // verdadero
Otra manera es conocida como Time-Based Blind, este provoca que la base de datos se detenga por un intervalo de tiempo como se muestra a continuación:

www.sitioweb.com/index.php?id=3 ‘ AND SLEEP(10)=’ //MYSQL
www.sitioweb.com/index.php?id=3 WAITFOR DELAY ’0:0:5′ //MSSQL

Figura 12. Ejemplo de Inyección SQL



Fuente: Samuel Esteban. 30 Jun. 2016 Inyección SQL: Definición y ejemplos reales. [consultado: 16 de noviembre de 2020] disponible en: https://backtrackacademy.com/articulo/inyeccion-sql-definicion-y-ejemplos

También se encuentra la inyección basada en errores; en inglés Error- Based que permite ver el error dentro del mismo sitio web
Y otros tipos de ataques de inyección como Union Query-Based y Stacked-queries

8.2.4 PREVENCIÓN DE ESTE ATAQUE

Para prevenir estos ataques es necesario establecer políticas de seguridad para el manejo de las bases de datos, restringiendo los privilegios de usuario y mantener una serie de prácticas normativas dentro de la organización como son las auditorías periódicas que dentro de los puntos principales a evaluar se integran monitoreo y pruebas que permiten identificar las falencias por medio de herramientas especiales, también se deben utilizar sentencias parametrizadas a manera de datos almacenados en variable y no como lenguaje SQL.[34]

8.2.5 ATAQUE Y SEGURIDAD DE SESION

"El atacante consigue el identificador de sesión entre una página web y un usuario, de forma que puede suplantar a este y acceder a su cuenta en la página web".

La forma como consiguen el identificador es por medio de ataque por fuerza bruta, tomando aleatoriamente hasta conseguir uno que les sea útil; robo por **sniffing**, mediante el uso de herramientas para interceptar tráficos de la red; otra forma es el robo por Cross-Site Scripting, por el historial del navegador y por robo en servidor compartido.

La manera de prevenir estos ataques es usando la función **session_save_path** y en general se debe limitar el tiempo de inactividad.

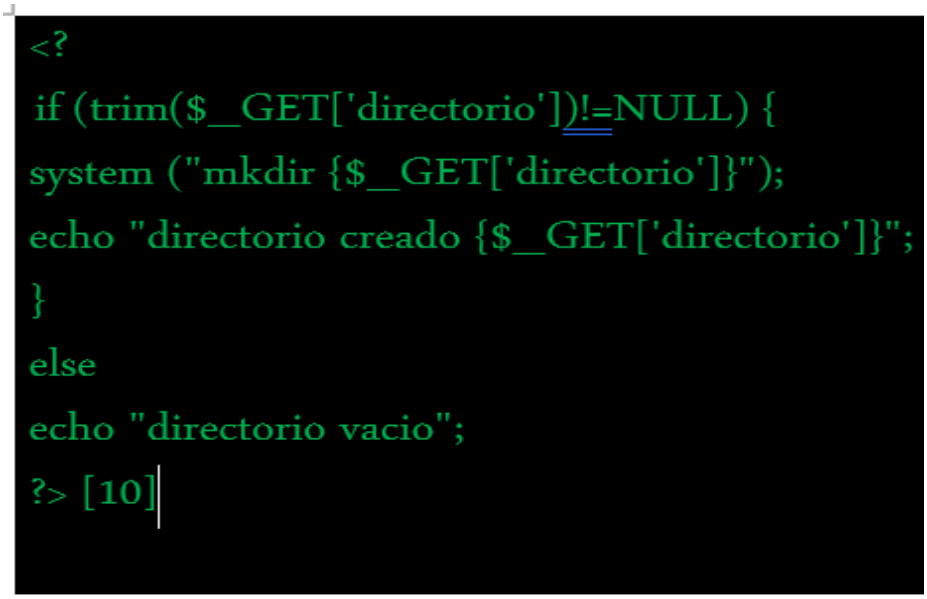
8.2.6 ATAQUE POR INYECCION DE COMANDOS EN PHP

Defectos en el desarrollo de aplicaciones con PHP lo cual se debe corregir validando correctamente la ejecución de comandos en el sistema.

Ejemplo: (Ver figura 13)

[34] SQLMap [sitio web] – Herramienta Automática de Inyección SQL. DragonJar [Consultado el 21 de abr. de 20]. Disponible en: https://www.dragonjar.org/sqlmap-herramienta-automatica-de-inyeccion-sql.xhtml

Figura 13. Ataque Ramsomware



Fuente: propia

8.2.8 ATAQUE RANSOMWARE

Este ataque se da por medio del puerto 27017 que trae la base de datos por defecto permitiendo al atacante tener acceso a la información.

Prevención de ransomware:

Para evitar el acceso no autorizado se deben tener en cuenta las configuraciones de los equipos y de las bases de datos y aplicaciones al ser instaladas ya que por descuido quedan los puertos por defecto, abiertos, que se convierten en el blanco de los atacantes.[35]

8.2.9 ATAQUE DoS

[35]SQLMap [sitio web]. Herramienta Automática de Inyección SQL. DragonJar [Consultado el 21 de abr. de 20]. Disponible en: https://www.dragonjar.org/sqlmap-herramienta-automatica-de-inyeccion-sql.xhtml

Ataque de denegación de servicio (DoS), para esto un atacante intenta evitar la legitimidad de que los usuarios accedan a información o a servicios del servidor.
El proceso que realiza es que "inunda" una red con información y el servidor solo puede procesar un límite de solicitudes de una vez por lo que entonces deniega el servicio. [13]
Para identificar un ataque de este tipo se puede observar el rendimiento de la red inusualmente lento (abrir archivos o acceder a sitios web), indisponibilidad de un sitio web en particular, incapacidad para acceder a cualquier sitio web y aumento en la cantidad de spam que recibimos.

8.3 ATAQUES EN SISTEMAS OPERATIVOS

Los sistemas operativos son muy atacados por ciberdelincuentes, y sus puntos críticos suelen ser las variables de interfaz, de usuarios y permisos por lo que es necesaria la implementación de políticas por medio de una serie de normas y chequeos que deben estar establecidos luego de un levantamiento del inventario equipos y verificación del medio en donde se encuentran, esto se logra siguiendo los pasos por alguna norma de seguridad como por ejemplo MAGERIT entre muchas más que se pueden adoptar para tomar las respectivas normas de seguridad.

Luego de evaluar las condiciones y estados de configuración que solo evalúan manualmente como es la interfaz y permisos del área donde se alojan los equipos se procede a las pruebas que pueden ser llevadas en un entorno de seguridad y control dentro de la organización y se llevan a cabo con diferentes herramientas tipo software con las que se identifican las vulnerabilidades existentes en los sistemas operativos tanto de Linux como de Windows
Existe un gran número de herramientas que se pueden utilizar según la necesidad y la variable a auditar o evaluar, con las que se realizan escaneos y pruebas de penetración al sistema y estas arrojan el nivel de criticidad en el que el sistema se encuentra y se mencionarán algunas a continuación.

Snort, es una herramienta basada en IDS, con la cual se pueden realizar escaneos al sistema operativo ya sea de Windows o Linux con el fin de encontrar las posibles vulnerabilidades en que este se encuentre.
Los riesgos en que se generalmente se encuentra un sistema son los agujeros que puede utilizar el atacante para entrar al sistema y son a través de los servicios que el servidor ofrece como son los puertos utilizados por este ya que muchas veces se encuentran con la configuración de fábrica.

Otra herramienta muy útil para escaneos y pruebas de penetración es nmap, con la que se pueden llevar a cabo evaluaciones en cuando a la asignación de permisos

al usuario o al administrador ya que un exceso de privilegios a este puede facilitar la tarea de robar información a un atacante en cuanto al acceso a los archivos y bases de datos alojadas en el sistema operativo.

También existen herramientas para la seguridad de sistemas operativos Windows como son los antivirus, entre estos el Panda que es muy útil para la protección en tiempo real.
Este puede escanear el sistema según se programe y además avisa al administrador sobre intentos de intrusión generando un informe completo de fecha y hora del evento.
Estas son solo algunas de muchas herramientas que pueden ser utilizadas para prevenir ataques y mantener la seguridad de los sistemas operativos.

ATAQUES OS FINGER PRINTING “huella digital del sistema operativo" / OS Finger Printing en Ethical Hacking son métodos que se utilizan para identificar de manera remota cual es el sistema operativo que se ejecuta y a partir de allí saber las formas de como penetrar dicho sistema. [36]

Toma de huellas de la pila activa: Es una tecnología con la que se puede determinar exactamente el sistema operativo de cada host dando la oportunidad de atacar con precisión el equipo destino.

Detección: Es posible detectar este ataque con el uso de herramientas como por ejemplo nmap.
Prevención: se puede prevenir o más bien minimizar el riesgo de este ataque con el uso de firewalls y /o proxis que dificultarían el acceso al S.O

TOMA DE HUELLA DE PILA PASIVA

Este tipo de ataque se lleva a cabo por medio del monitoreo de red para identificar o determinar el sistema operativo en uso olfateando el sistema en relación con los sniffer como puede ser wirwshark o snort.

Prevención: Una de las técnicas para evitar este tipo de ataque es implementando un sistema de detección de intruso IDS, aunque cabe recordar que muchas veces no es efectivo debido a que no es reactivo. De otra forma es, enmascarando el sistema o cambiando la configuración TCP/IP o engañando al atacante con sistemas operativos virtuales que ocultarían al S.O real.

KEYLOGGERS

[36] RUBEN.Ramiro. [en linea]. 25 tipos de ataques informáticos y cómo prevenirlos. ciberseguridad.blog: ENERO 20 de 2018. 25 tipos de ataques informáticos y cómo prevenirlos. [consultado el 2 de may. de 20] disponible en: https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

Consiste en utilizar un hardware o un software con el fin de registrarla actividad en el teclado de usuarios para conseguir contraseñas de todas las cuentas administradas por dicho usuario.
Este ataque se genera por descarga o clic en ventanas con enlaces maliciosos.

Detección: por este ataque de tipo malware no existe una herramienta o programa que permita su detección.

Prevención: Es posible prevenirlo con un software antivirus en tiempo real y para más protección se pueden usar programas como por ejemplo el Zenmap AntiLogger y SpyShelter Stop-Logger que permiten cifrar las pulsaciones del teclado.

8.3.1 ATAQUES A LINUX

ATAQUES DDOS

Son lanzados por medio de infecciones de iptables en sistemas operativos Linux dirigidos por sus servidores web tomando el control de manipulación remota de los sistemas o mejor explicado; por medio del envío de paquetes falsificados a la máquina objetivo obligado a no estar disponible para la validación de usuarios.

La prevención de estos ataques se realiza con el uso de herramientas como snort y con el uso de iptables y la tecnología de Network IDS.

8.4 ATAQUES SERVIDORES WEB

La forma de cómo se presenta es con un inicio de sesión remota a través de ssh o servicios HTTP a través de los cuales pueden los delincuentes obtener los mapas de la red y pueden causar un desbordamiento de buffer por el uso de valores arbitrarios debido a que así pueden encontrar el control administrativo completo

La forma de cómo prevenirlo es cerrando el puerto preestablecido de fábrica.

8.4.1 IP SPOOFING (ENGAÑO DE IPS)

Este ataque se desarrolla a través de un programa o un caballo de troya con el fin de lograr controlar la red aprovechando la vulnerabilidad de los servidores, dependiendo de los servicios que se ejecuten el sistema como por ejemplo los **rsh**,

telnet y otros más y es posible con el uso de herramientas por los piratas para alcanzar el objetivo.

8.4.2 EAVESDROPPING (BAJAR LOS ALEROS)

Se basa en reunir los datos que pasan entre dos nodos por medio del rastreo de su respectiva conexión.
Se desarrolla por medio de los protocolos de transmisión de texto plano como por ejemplo el FTP y el HTTP.[37]

Prevención: Se puede evitar implementando un servicio que encripta las llaves que se intercambian, generando contraseñas que solo sirven para una sola sesión y encriptación de transmisión.

8.5 HERRAMIENTAS PARA REALIZAR ATAQUES A BASES DE DATOS Y EXPLORAR VULNERAVILIDADES EN ENTORNO DE PRUEBAS

Existe un gran número de aplicaciones que son útiles para realizar auditorías y detectar vulnerabilidades en bases de datos y son empleadas según la necesidad de identificación o la complejidad del sistema.
Pero, este gran número de herramienta también son utilizados por delincuentes para atacar las bases de datos de manera ilegal con el fin de tener beneficios propios como puede ser intereses financieros, por ejemplo.
Algunas de esas aplicaciones se mencionan a continuación:

- ✔ SQLIer
- ✔ SQLibf
- ✔ SQLBrute
- ✔ BobCat
- ✔ SQLMap
- ✔ SQLNinja

Todas con el fin de realizar ataques de inyección SQL, a través de escaneos ip, url o por puertos entre otras funciones que permiten lograr identificar los huecos existentes en las bases de datos que mayor mente se dan por mala configuración y lograr penetrar dicho sistema.[38]

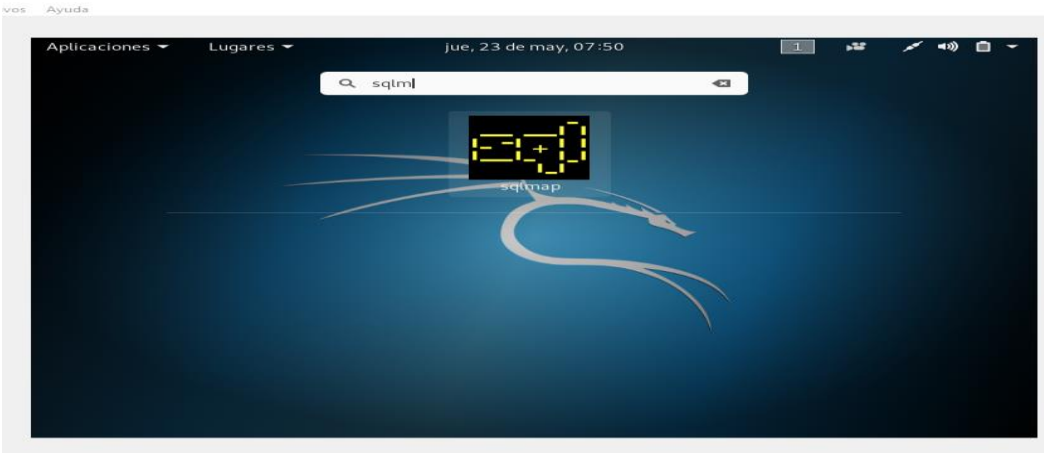
---

[37] red hat enterprise linux [en linea]. manual de seguridad
copyright © 2005 por red hat, inc [consultado: 2 de may. de 20]. disponible en: http://web.mit.edu/rhel-doc/4/rh-docs/pdf/rhel-sg-es.pdf

[38] herramientas sql injection.. publicado por vicente motos on martes, 26 de agosto de 2008 etiquetas: herramientas [en línea] [consultado mayo 23] disponible en: https://www.hackplayers.com/2008/08/herramientas-sql-injection.html

Ejemplos de ataque a sistemas de bases de datos con SQLMap, con esta herramienta se realizan inyecciones SQL de forma automatizada y se encuentra integrada en kali Linux como se observa en la figura 2

Figura 14. *Imagen Sqlmap*

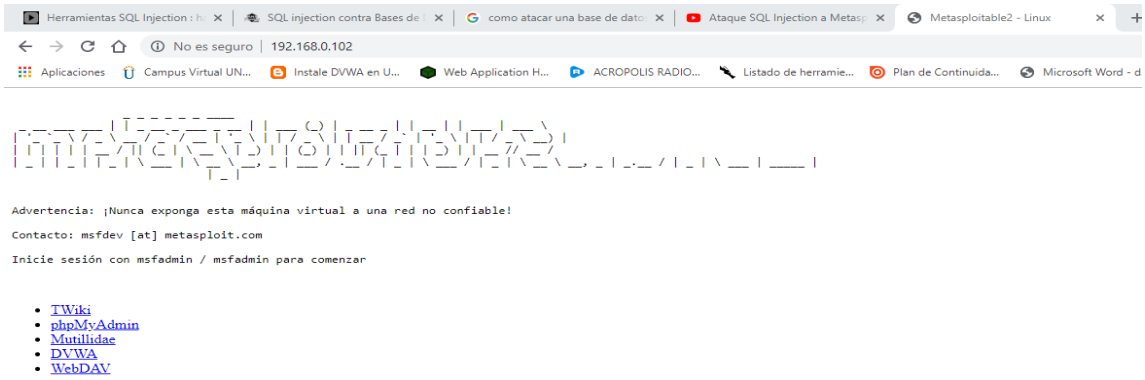


Fuente: Propia

Para el desarrollo del ataque se debe identificar el objetivo, ya sea con una dirección ip o una dirección url.

A continuación se muestra un ataque en entorno de pruebas con sqlmap contra las base de datos en metasploitable 2

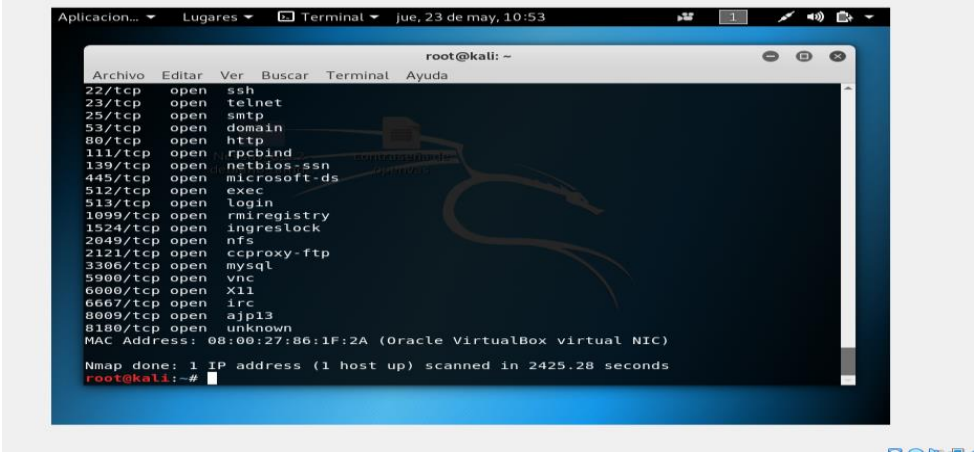
Figura 15. Ataques de bases de Datos con Sqlmap



Fuente: Hernandez Contreras, Nancy Janeth. Mayo, 2019.
Ataques a bases de datos, Articulo Fase 5 - Laboratorio de bases de datos- especialización seguridad informática.

Para este caso se verifica los puertos utilizados con la herramienta de escaneo nmap por medio del comando ***nmap –s S “dirección ip”***
Y se puede observar que el puerto utilizado por mysql es el 3306

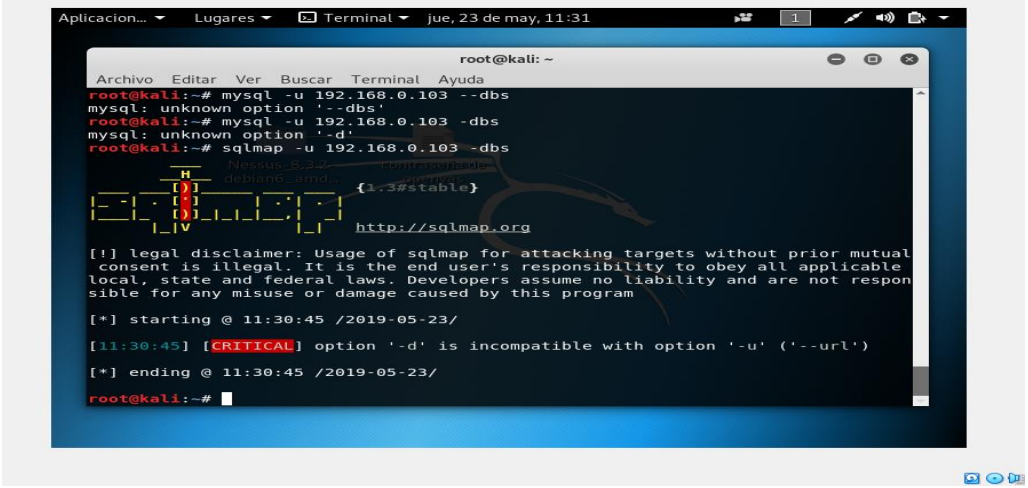
Figura 16. Imagen de Laboratorio de ataques a Bases de Datos



Fuente: Hernandez Contreras, Nancy Janeth. Mayo, 2019.
Ataques a bases de datos, Articulo Fase 5 - Laboratorio de bases de datos- especialización en seguridad informática.

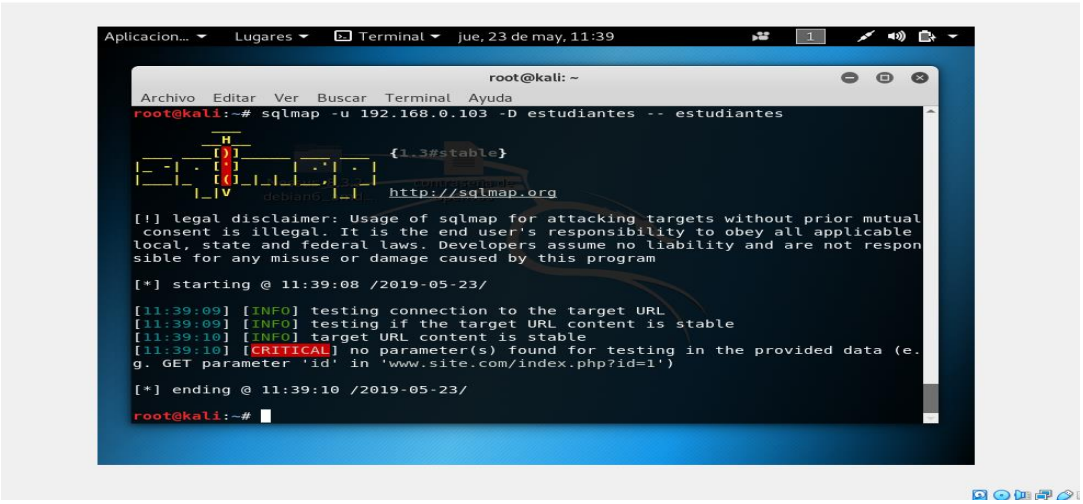
O también se puede acceder directamente con sqlmap
Con el comando sqlmap –u “dirección ip” –dbs
Lo cual mostrará algo como se muestra en la figura siguiente:

Figura 17. *Ataques de bases de Datos con Sqlmap*



Fuente: Hernandez Contreras, Nancy Janeth. Mayo, 2019.

Figura 18. Ataques de Bases de Datos con Sqlmap en entorno de pruebas



Fuente: Hernández Contreras, Nancy Janeth. Mayo, 2019.
Ataques a bases de datos, Articulo Fase 5 - Laboratorio de bases de datos- especialización en seguridad informática.

Este es solo un ejemplo entre diferentes formas de ataque y uso de herramientas que pueden ser usadas para tal fin, por eso es necesario mantener las políticas de seguridad en los sistemas informáticos y en el uso dispositivos, plataformas, o cuentas en las que se almacenarían las copias digitales de archivos o documentos a proteger y conservar.

9 PROCEDIMIENTOS DE LA GESTIÓN DE RIESGOS UTILIZANDO LA METODOLOGÍA MAGERIT Y CONTROLES DE LA ISO 27001:2013

Para realizar el análisis y la gestión de riesgos requieren de información de la entidad la cual se intervendrá, con el fin de establecer en qué estado se encuentra la infraestructura tecnológica y de operación, de la seguridad de la información y cumplimiento normativo.

"El Modelado de Amenazas de Seguridad es un proceso para la evaluar y documentar los riesgos de seguridad de un sistema. A continuación, se muestra un ejemplo de modelado donde se identifican amenazas que comprometen la seguridad de un sistema en entidades y los respectivos controles ante cada riesgo que se presenta".[39]

9.1 IDENTIFICACIÓN DE LOS ACTIVOS, AMENAZAS, VULNERABILIDADES Y SALVAGUARDAS.

Tabla 1. Análisis de Riesgos.

Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	Salvaguarda
[HW] Equipo de computo	[A25] Robo	Falta de controles de entrada y salida de los recursos del sistema.	Se identifican y establecen medidas de control físicas con el fin de proteger de manera correcta cada activo de información y así evitar incidentes que comprometan la integridad física de la información o interferencias no deseadas.

[39] INCIBE. Análisis de riesgos en 6 pasos Seguridad y auditoria de sistemas. [sitio web] incibe.es: 01 de junio de 2017.. [consultado: 4 de mayo de 2020] Disponible en: https://www.incibe.es/en/node/2789

Continuación Tabla 1. Análisis de Riesgos			
[HW] Switch	[A4] Manipulación de la configuración	Alteraciones por personal no capacitado en las configuraciones del dispositivo	Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.
[HW] Teléfono ip	[I8] Fallo de servicios de comunicaciones	La desconfiguración es común	Minimizar las fallas de los equipos de comunicación con la respectiva configuración de los dispositivos.
[HW] Impresora	[I5] Avería de origen físico o lógico	Errores de solicitudes de impresiones	Ingresar mediante la IP a las impresoras y supervisar el estado de las impresiones en cada departamento de la institución.
[HW] Servidor FTP	[A11] Acceso no autorizado	Alteraciones por personal no capacitado en las configuraciones del dispositivo.	Establecer, documentar y revisar la política de control de acceso periódicamente, lo que significa que una política documentada es obligatoria.
[HW] Servidor DHCP	[A11] Acceso no autorizado	Sistema estructural de protección de los recursos del sistema contra eventualidades ocasionadas por el agua.	Establecer, documentar y revisar la política de control de acceso periódicamente, lo que significa que una política documentada es obligatoria.

Continuación Tabla 1. Análisis de Riesgos			
[HW] Servidor del Sistema de Registro y Control	[A19] Divulgación de información	Falta de controles de entrada y salida de los recursos del sistema.	Establece un proceso formal para asignar y revocar los accesos a sistemas y servicios.
[HW] Servidor PBX	[I2] Daños por agua	Alteraciones por personal no capacitado en las configuraciones del dispositivo.	Cuando la información se transfiere a través de redes públicas o redes inalámbricas, se deben considerar controles adicionales para mantener las conexiones (disponibilidad) y la privacidad (confidencialidad) y la integridad de los datos.
[HW] Firewall	[A11] Acceso no autorizado	Sistema estructural de protección de los recursos del sistema contra eventualidades ocasionadas por el agua.	Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.
[HW] Router	[I6] Corte del suministro eléctrico	Falta de controles de entrada y salida de los	Asegurar la protección de la información en redes y la protección de la

		recursos del sistema.	infraestructura de soporte.
Continuación Tabla 1. Análisis de Riesgos			
[COM] Hub	[A4] Manipulación de la configuración	Alteraciones por personal no capacitado en las configuraciones del dispositivo	Se identifican y establecen medidas de control físicas con el fin de proteger de manera correcta cada activo de información y así evitar incidentes que comprometan la integridad física de la información o interferencias no deseadas.
[S] Internet	[I6] Corte del suministro eléctrico	Sistema estructural de protección de los recursos del sistema contra eventualidades ocasionadas por el agua.	Cuando la información se transfiere a través de redes públicas o redes inalámbricas, se deben considerar controles adicionales para mantener las conexiones (disponibilidad) y la privacidad (confidencialidad) y la integridad de los datos.

Continuación Tabla 1. Análisis de Riesgos			
[S] Almacenamiento página web	[A4] Manipulación de la configuración	Sistema estructural de protección de los recursos del sistema contra eventualidades ocasionadas altas en el fluido eléctrico	Las políticas y los procedimientos deben incluir requisitos para la protección contra intercepción, copia, modificación, dirección incorrecta o destrucción. Esto debe estar respaldado por políticas de uso aceptable, una política que cubra el manejo de archivos adjuntos, el uso de encriptación y cualquier seudonimización de datos.

Continuación Tabla 1. Análisis de Riesgos			
[S] Almacenamiento de sitios	[A4] Manipulación de la configuración	Falta de controles de entrada y salida de los recursos del sistema.	Las políticas y los procedimientos deben incluir requisitos para la protección contra intercepción, copia, modificación, dirección incorrecta o destrucción. Esto debe estar respaldado por políticas de uso aceptable, una política que cubra el manejo de archivos adjuntos, el uso de encriptación y cualquier seudonimización de datos.
[S] Almacenamiento de sitios	[A11] Acceso no autorizado	Alteraciones por personal no capacitado en las configuraciones del dispositivo	Las políticas y los procedimientos deben incluir requisitos para la protección contra intercepción, copia, modificación, dirección incorrecta o destrucción. Esto debe estar respaldado por políticas de uso aceptable, una política que cubra el manejo de archivos adjuntos, el uso de encriptación y cualquier seudonimización de datos.

Continuación Tabla 1. Análisis de Riesgos			
[SW] Apache 2.4.25	[E20] Vulnerabilidades de los programas (software)	Sistema estructural de protección de los recursos del sistema contra eventualidades ocasionadas por el agua.	implementar capacitaciones de formación y concienciación sobre los procesos para el tratamiento de la información y el respectivo cuidado o seguridad.
[SW] PHP 5.6.30	[E20] Vulnerabilidades de los programas (software)	Sistema estructural de protección de los recursos del sistema contra eventualidades ocasionadas altas en el fluido eléctrico	implementar capacitaciones de formación y concienciación sobre los procesos para el tratamiento de la información y el respectivo cuidado o seguridad.
[SW] MySQL 5.7.17	[E20] Vulnerabilidades de los programas (software)	Fallas en el sistema de identificación y autorización en los recursos del sistema.	implementar capacitaciones de formación y concienciación sobre los procesos para el tratamiento de la información y el respectivo cuidado o seguridad.
[SW] phpMyAdmin 4.6.6	[E20] Vulnerabilidades de los programas (software)	Fallas en el sistema de identificación y autorización en los recursos del sistema.	implementar capacitaciones de formación y concienciación sobre los procesos para el tratamiento de la información y el respectivo cuidado o seguridad.
[SW] Windows 10	[E21] Errores de mantenimiento / actualización de programas (software)	Fallas en el control de seguridad de la información	implementar capacitaciones de formación y concienciación sobre los procesos

Continuación Tabla 1. Análisis de Riesgos			
			para el tratamiento de la información y el
			respectivo cuidado o seguridad.

40

Tratamiento de los riesgos según evaluación
Estos pueden ser:

- Eliminados
- Trasferidos
- Aceptados o
- Mitigados

Tabla 2. Tratamiento de Riesgos

Amenazas Metodología Magerit	**Vulnerabilidades**	**SUPERACIÓN DEL RIESGO**	**DESCRIPCIÓN**
[A11] Acceso no autorizado	Acceso físico no protegido a las oficinas o establecimiento	**ELIMINAR**	Eliminar el acceso a usuarios a sistemas y bases de datos

[40] MAGERIT v.3 . [en linea] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [consultado: 5 de mayo de 2020] disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Continuación Tabla 2. Tratamiento de Riesgos			
[A11] Acceso no autorizado	Acceso físico no protegido a las oficinas o establecimiento	**IMPLANTAR**	eliminar el acceso a usuarios no autorizados a sistemas y bases de datos
[A24] Denegación de servicio	Falta de filtros que protejan al sistema contra saturaciones	**ELIMINAR**	instalar software antivirus con sus respectivas licencias por un año
[A24] Denegación de servicio	Falta de filtros que protejan al sistema contra saturaciones	**IMPLANTAR**	instalar software antivirus con sus respectivas licencias por un año
[A5] Suplantación de la identidad del usuario	Posibilidad de gestionar el sistema en forma remota	**IMPLANTAR**	Para mitigarlo, el sistema se debe fortalecerse a través de un procedimiento de acceso más seguro para los usuarios tal como la implementación de captchas y exigencia de contraseñas más robustas.

Continuación Tabla 2. Tratamiento de Riesgos

[A5] Suplantación de la identidad del usuario	Los recursos compartidos facilitan el uso del sistema por parte de personas no autorizadas	**IMPLANTAR**	Para mitigarlo, el sistema se debe fortalecer a través de un procedimiento de acceso más seguro para los usuarios tal como la implementación de captchas y exigencia de contraseñas más robustas.
[A5] Suplantación de la identidad del usuario	Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	**ELIMINAR**	Se debe limitar y controlar los puertos de acceso remoto a los usuarios.
[A5] Suplantación de la identidad del usuario	Los recursos compartidos facilitan el uso del sistema por parte de personas no autorizadas	**ELIMINAR**	Se debe limitar y controlar el acceso de los usuarios a los sistemas y bases de datos.
[A6] Abuso de privilegios de acceso	Ingreso del personal de prácticas de otras dependencias para alimentar sistema	**ELIMINAR**	Se debe limitar y controlar el acceso de los usuarios a los sistemas y bases de datos.

Continuación Tabla 2. Tratamiento de Riesgos

[A7] Uso no previsto	Utilización de los recursos del sistema para fines no previstos	**ELIMINAR**	Se debe limitar y controlar el acceso de los usuarios a los sistemas y bases de datos.
[A8] Difusión de software dañino	Falta de políticas de antivirus	**TRANSFERIR**	Se debe contratar un servicio de antivirus y seguridad de sistemas.
[E14] Escapes de información	Falta de protección de las copias de seguridad	**ELIMINAR**	Se debe limitar y controlar el acceso de los usuarios a las bases de datos y copias de seguridad.
[E15] Alteración accidental de la información	Ingreso del personal de prácticas de otras dependencias para alimentar sistema	**ELIMINAR**	Se debe limitar y controlar el acceso de los usuarios a los sistemas y bases de datos.

Continuación Tabla 2. Tratamiento de Riesgos

[E18] Destrucción de información	Ingreso del personal de prácticas de otras dependencias para alimentar sistema	**ELIMINAR**	Se debe limitar y controlar el acceso de los usuarios a los sistemas y bases de datos.
[E18] Destrucción de información	Manipulación de la información por practicantes de otras dependencias	**ELIMINAR**	Se debe limitar y controlar el acceso de los usuarios a los sistemas y bases de datos.
[E19] Fugas de información	Revelación de información por el personal de prácticas de otras dependencias indiscretamente	**ELIMINAR**	Se debe limitar y controlar el acceso de los usuarios a los sistemas y bases de datos.
[E2] Errores del administrador	Faltan normas técnicas de filtrado	**IMPLANTAR**	Instalar alternativas para evitar el riesgo.
[E21] Errores de mantenimiento / actualización de programas (software)	Uso de una versión obsoleta de las aplicaciones	**IMPLANTAR**	Comprar e instalar el software necesario para evitar el riesgo.
[E21] Errores de mantenimiento / actualización de programas (software)	Uso de una versión obsoleta de las aplicaciones o componentes del sistema 0	**IMPLANTAR**	Comprar e instalar el software necesario para evitar el riesgo.

Continuación Tabla 2. Tratamiento de Riesgos

[E21] Errores de mantenimiento / actualización de programas (software)	Uso de una versión obsoleta de las aplicaciones o componentes del sistema operativo	**IMPLANTAR**	Comprar e instalar el software necesario para evitar el riesgo.
[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de informes de las operaciones de mantenimiento	**IMPLANTAR**	Comprar e instalar el software necesario para evitar el riesgo.
[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de informes de las operaciones de mantenimiento	**IMPLANTAR**	Implementar un registro para documentar e informar las operaciones de mantenimiento.
[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de informes de las operaciones de mantenimiento	**IMPLANTAR**	Implementar un registro para documentar e informar las operaciones de mantenimiento.
[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de informes de las operaciones de mantenimiento	**IMPLANTAR**	Implementar un registro para documentar e informar las operaciones de mantenimiento.
[E23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de informes de las operaciones de mantenimiento	**IMPLANTAR**	Implementar un registro para documentar e informar las operaciones de mantenimiento.

Continuación Tabla 2. Tratamiento de Riesgos

[E28] Indisponibilidad del personal	Ausencia del puesto de trabajo por enfermedad	**IMPLANTAR**	Se debe implementar alternativas de Seguridad y Salud en el Trabajo.
[E9] Errores de [re-]encaminamiento	Hay un solo segmento de red	**IMPLANTAR**	Se debe realizar la debida segmentación de la red y aplicación de VLAN para proteger las LAN sensibles.
[I11] Emanaciones electromagnéticas	Hardware sensible a las emisiones electromagnéticas (restaurante y cocina)	**ASUMIR**	Instalar alternativas para evitar el riesgo.
[I7] Condiciones inadecuadas de temperatura o humedad	Falta de hardware redundante	**TRANSFERIR**	Se debe contratar un servicio para la instalación de aires acondicionados y sistemas de refrigeración para la protección de los equipos de cómputo y así perduren unos días más en la empresa
[I7] Condiciones inadecuadas de temperatura o humedad	Necesita climatización para funcionar	**TRANSFERIR**	Se debe contratar un servicio para la instalación de aires acondicionados y sistemas de refrigeración para la protección de los equipos de cómputo y así perduren unos días más en la empresa

Continuación Tabla 2. Tratamiento de Riesgos

[I7] Condiciones inadecuadas de temperatura o humedad	Falta de hardware redundante	**TRANSFERIR**	Se debe contratar un servicio para la instalación de aires acondicionados y sistemas de refrigeración para la protección de los equipos de cómputo y así perduren unos días más en la empresa
[I7] Condiciones inadecuadas de temperatura o humedad	Necesita climatización para funcionar	**TRANSFERIR**	Se debe contratar un servicio para la instalación de aires acondicionados y sistemas de refrigeración para la protección de los equipos de cómputo y así perduren unos días más en la empresa

Continuación Tabla 2. Tratamiento de Riesgos

[I7] Condiciones inadecuadas de temperatura o humedad	Falta de hardware redundante	**TRANSFERIR**	Contratar un servicio para la instalación de aires acondicionados y sistemas de refrigeración para la protección de los equipos de cómputo y así perduren unos días más en la empresa
[I7] Condiciones inadecuadas de temperatura o humedad	Falta de hardware redundante	**IMPLANTAR**	contratar un servicio para la instalación de aires acondicionados y sistemas de refrigeración para la protección de los equipos de cómputo y así perduren unos días más en la empresa
[I7] Condiciones inadecuadas de temperatura o humedad	Necesita climatización para funcionar	**ELIMINAR**	contratar un servicio para instalación de aires acondicionados y sistemas de refrigeración para la protección de los equipos.
[I8] Fallo de servicios de comunicaciones	Acceso físico no protegido a los locales que alojan equipos	**ASUMIR**	Limitar y controlar el acceso de los usuarios a los sistemas y bases de datos.

41

41 MAGERIT v.3 [en linea]. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [consultado: 5 de mayo de 2020] disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

SISTEMA DE CONTROL INTERNO INFORMÁTICO

El Control Interno Informático es el sistema integrado al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el propósito de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos automatizados.

Controles de la ISO 27001:2013

Equipo de cómputo. Controles por establecer:

A11 Seguridad física y del entorno.

A11.1 Áreas de seguridad. Restringir accesos físicos sin debida autorización, daños e interrupciones contra las instalaciones y/o recursos de procesamiento de información.
A11.1.2 Controles de acceso físico. Aquellas áreas que la organización considera seguras deben estar blindadas por controles de entrada que permitan solo personal autorizado.

A11.1.3 Seguridad de oficinas, despachos e instalaciones. Deben implementarse para evitar el riesgo que la información confidencial y privada sea accesible para los terceros.

A11.1.4 Protección contra amenazas externas y del ambiente. Teniendo en cuenta las situaciones externas e inestables que a diario se viven y de un clima impredecible, se debe considerar, diseñar y establecer la protección física contra factores externos.

11.2 Seguridad de los equipos. Los daños ocasionados en los equipos pueden causar dificultades y entorpecimientos en la actividad de la organización o en su defecto vulnerar la confidencialidad de la información causada por robos de activos.

11.2.1 Ubicación y protección del equipamiento. Debe evitarse accesos no autorizados, medidas de protección contra daños eléctricos, establecerse pautas para actividades no permitidas comer, beber y fumar cerca a los equipos para evitar daños o que los funcionarios permanezcan en contacto con los equipos si no están trabajando en ellos.

11.2.3 Seguridad en el cableado. Controles para protección del cableado de energía y de comunicaciones que posiblemente pueda afectar los sistemas de información.

11.2.4 Mantenimiento del equipamiento. Los controles para garantizar que los equipos se mantienen adecuadamente para garantizar que no se deterioren y estén siempre disponibles.

11.2.8 Equipamiento desatendido por el usuario. Se recomienda que los usuarios no deban dejar las sesiones abiertas mientras el equipo no esté atendido.

Switch. Controles por establecer:

A13 Seguridad en las comunicaciones.

A13.1 Gestión de la seguridad de red.

A13.1.1 Controles de red. Para gestionar una red se debe asegurar de que se han asignado responsabilidades dentro del equipo de gestión y que se siguen una serie de procedimientos establecidos.

13.1.2 Seguridad de los servicios de red. Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.

13.1.3 Separación en redes. Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.

Servidor FTP. Controles por establecer:
A9. Control de acceso.

A9.1 Requisitos generales para el control de acceso. Están enfocadas a controlar y monitorizar los accesos a los medios de información de acuerdo a las políticas definidas por la organización.

A9.1.1 Política de control de acceso. Define las reglas de control de acceso a la información, osea los derechos y restricciones de acceso a la información.

A9.1.2 Gestión de acceso a los usuarios. Determina los requisitos para gestionar la autorización de los usuarios que acceden a los recursos de red.

A9.2 Gestión del acceso de usuarios. Controles para garantizar que solamente los usuarios autorizados acceden a los sistemas y servicios.

9.2.2 Gestión de acceso a los usuarios. Establece un proceso formal para asignar y revocar los accesos a sistemas y servicios.

9.2.3 Gestión de derechos de acceso privilegiados. Debe realizarse de forma independiente mediante un proceso específico que tenga en cuenta las políticas de acceso privilegiado definidas.

9.2.4 Gestión de la información de autenticación secreta de los usuarios. Control para garantizar que se mantiene la confidencialidad de la información secreta de acceso.
9.2.5 Revisión de derechos de acceso de usuario. Control para establecer una revisión periódica de los permisos de accesos de los usuarios.

9.2.6 Remoción o ajuste de los derechos de acceso. Control para garantizar que se modifican los derechos de acceso.

A9.3 Responsabilidades del usuario. Control donde los usuarios son responsables de mantener a salvo sus contraseñas o información de autenticación.

9.3.1 Uso de la información de autenticación secreta. Establecer normas para la utilización de contraseñas basándose en asegurar que las contraseñas no se divulguen.

A9.4 Control de acceso al sistema y a las aplicaciones. Prevenir accesos no autorizados a sistemas y aplicaciones.

9.4.1 Restricción del acceso a la información. Las funciones de una aplicación o sistema deben considerar las restricciones de control de acceso determinadas por la política de control definido.

9.4.2 Procedimientos de conexión (log-on) seguros. Control para establecer inicios de sesión seguros.

9.4.3 Sistema de gestión de contraseñas. Los sistemas de administración deben aplicar contraseñas de calidad, rechazar contraseñas débiles, requerir confirmación y, si se emiten con ID, forzar el cambio de las contraseñas en el primer inicio de sesión.

9.4.5 Control de acceso al código de programas fuente. El código fuente debe estar protegido con acceso restringido mediante el uso de librerías fuente.

Servidor DHCP. Controles para establecer:

A9. Control de acceso.

A9.1 Requisitos generales para el control de acceso. Están enfocadas a controlar y monitorizar los accesos a los medios de información de acuerdo con las políticas definidas por la organización.

A9.1.1 Política de control de acceso. Define las reglas de control de acceso a la información, o sea los derechos y restricciones de acceso a la información.

A9.1.2 Gestión de acceso a los usuarios. Determina los requisitos para gestionar la autorización de los usuarios que acceden a los recursos de red.

A9.2 Gestión del acceso de usuarios. Controles para garantizar que solamente los usuarios autorizados acceden a los sistemas y servicios.

9.2.2 Gestión de acceso a los usuarios. Establece un proceso formal para asignar y revocar los accesos a sistemas y servicios.

9.2.3 Gestión de derechos de acceso privilegiados. Debe realizarse de forma independiente mediante un proceso específico que tenga en cuenta las políticas de acceso privilegiado definidas.

9.2.4 Gestión de la información de autenticación secreta de los usuarios. Control para garantizar que se mantiene la confidencialidad de la información secreta de acceso.

9.2.5 Revisión de derechos de acceso de usuario. Control para establecer una revisión periódica de los permisos de accesos de los usuarios.

9.2.6 Remoción o ajuste de los derechos de acceso. Control para garantizar que se modifican los derechos de acceso.

A9.3 Responsabilidades del usuario. Control donde los usuarios son responsables de mantener a salvo sus contraseñas o información de autenticación.

9.3.1 Uso de la información de autenticación secreta. Establecer normas para la utilización de contraseñas basándose en asegurar que las contraseñas no se divulguen.

A9.4 Control de acceso al sistema y a las aplicaciones. Prevenir accesos no autorizados a sistemas y aplicaciones.

9.4.1 Restricción del acceso a la información. Las funciones de una aplicación o sistema deben considerar las restricciones de control de acceso determinadas por la política de control definido.

9.4.2 Procedimientos de conexión (log-on) seguros. Control para establecer inicios de sesión seguros.

9.4.3 Sistema de gestión de contraseñas. Los sistemas de administración deben aplicar contraseñas de calidad, rechazar contraseñas débiles, requerir confirmación y, si se emiten con ID, forzar el cambio de las contraseñas en el primer inicio de sesión.

9.4.5 Control de acceso al código de programas fuente. El código fuente debe estar protegido con acceso restringido mediante el uso de librerías fuente.

Servidor del sistema de registro y control. Controles por establecer:

A9. Control de acceso.

A9.1 Requisitos generales para el control de acceso. Están enfocadas a controlar y monitorizar los accesos a los medios de información de acuerdo a las políticas definidas por la organización.

A9.1.1 Política de control de acceso. Define las reglas de control de acceso a la información, o sea los derechos y restricciones de acceso a la información.

A9.1.2 Gestión de acceso a los usuarios. Determina los requisitos para gestionar la autorización de los usuarios que acceden a los recursos de red.

A9.2 Gestión del acceso de usuarios. Controles para garantizar que solamente los usuarios autorizados acceden a los sistemas y servicios.

9.2.2 Gestión de acceso a los usuarios. Establece un proceso formal para asignar y revocar los accesos a sistemas y servicios.

9.2.3 Gestión de derechos de acceso privilegiados. Debe realizarse de forma independiente mediante un proceso específico que tenga en cuenta las políticas de acceso privilegiado definidas.

9.2.4 Gestión de la información de autenticación secreta de los usuarios. Control para garantizar que se mantiene la confidencialidad de la información secreta de acceso.

9.2.5 Revisión de derechos de acceso de usuario. Control para establecer una revisión periódica de los permisos de accesos de los usuarios.

9.2.6 Remoción o ajuste de los derechos de acceso. Control para garantizar que se modifican los derechos de acceso.

A9.3 Responsabilidades del usuario. Control donde los usuarios son responsables de mantener a salvo sus contraseñas o información de autenticación.

9.3.1 Uso de la información de autenticación secreta. Establecer normas para la utilización de contraseñas basándose en asegurar que las contraseñas no se divulguen.

A9.4 Control de acceso al sistema y a las aplicaciones. Prevenir accesos no autorizados a sistemas y aplicaciones.

9.4.1 Restricción del acceso a la información. Las funciones de una aplicación o sistema deben considerar las restricciones de control de acceso determinadas por la política de control definido.

9.4.2 Procedimientos de conexión (log-on) seguros. Control para establecer inicios de sesión seguros.

9.4.3 Sistema de gestión de contraseñas. Los sistemas de administración deben aplicar contraseñas de calidad, rechazar contraseñas débiles, requerir confirmación y, si se emiten con ID, forzar el cambio de las contraseñas en el primer inicio de sesión.

9.4.5 Control de acceso al código de programas fuente. El código fuente debe estar protegido con acceso restringido mediante el uso de librerías fuente.

Firewall. Controles por establecer:

A13 Seguridad en las comunicaciones.

A13.1 Gestión de la seguridad de red.

A13.1.1 Controles de red. Para gestionar una red se debe asegurar de que se han asignado responsabilidades dentro del equipo de gestión y que se siguen una serie de procedimientos establecidos.

13.1.2 Seguridad de los servicios de red. Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.

13.1.3 Separación en redes. Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.

Router. Controles por establecer:

A13 Seguridad en las comunicaciones.

A13.1 Gestión de la seguridad de red.

A13.1.1 Controles de red. Para gestionar una red se debe asegurar de que se han asignado responsabilidades dentro del equipo de gestión y que se siguen una serie de procedimientos establecidos.

13.1.2 Seguridad de los servicios de red. Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.

13.1.3 Separación en redes. Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.

Hub. Controles para establecer:

A11 Seguridad física y del entorno.

A11.1 Áreas de seguridad. Restringir accesos físicos sin debida autorización, daños e interrupciones contra las instalaciones y/o recursos de procesamiento de información.

A11.1.2 Controles de acceso físico. Aquellas áreas que la organización considera seguras deben estar blindadas por controles de entrada que permitan solo personal autorizado.

11.2 Seguridad de los equipos. Los daños ocasionados en los equipos pueden causar dificultades y entorpecimientos en la actividad de la organización o en su defecto vulnerar la confidencialidad de la información causada por robos de activos.

11.2.1 Ubicación y protección del equipamiento. Debe evitarse accesos no autorizados, medidas de protección contra daños eléctricos, establecerse pautas para actividades no permitidas comer, beber y fumar cerca a los equipos para evitar daños o que los funcionarios permanezcan en contacto con los equipos si no están trabajando en ellos.

11.2.4 Mantenimiento del equipamiento. Los controles para garantizar que los equipos se mantienen adecuadamente para garantizar que no se deterioren y estén siempre disponibles.

Almacenamiento de la página web. Controles para establecer:

A13 Seguridad en las comunicaciones.

A13.2 Intercambio de información. Requisitos o controles para proteger la información cuando se transmiten datos bien sea internamente o entre varias entidades.

13.2.1 Políticas y procedimientos de intercambio de información. Definir procedimientos y políticas para proteger la información que se va a transmitir donde se tenga en cuenta todos los aspectos.

13.2.2 Acuerdos de intercambio de información. Deben existir acuerdos entre las partes de intercambio de información para garantizar tanto el uso que se le va a dar a la información como los niveles de protección.

13.2.3 Mensajería electrónica. El correo electrónico debe ser tratado como un activo más de información donde se apliquen controles apropiados para mantener la confidencialidad, Integridad y disponibilidad de la información.

13.2.4 Acuerdos de confidencialidad y de no divulgación. Se deben considerar acuerdos de confidencialidad tanto a personal propio como a clientes y proveedores si tiene acceso a activos de información que así lo requieran.

Almacenamiento de sitos. Controles que establecer:

A13 Seguridad en las comunicaciones.

A13.2 Intercambio de información. Requisitos o controles para proteger la información cuando se transmiten datos bien sea internamente o entre varias entidades.

13.2.1 Políticas y procedimientos de intercambio de información. Definir procedimientos y políticas para proteger la información que se va a transmitir donde se tenga en cuenta todos los aspectos.

13.2.2 Acuerdos de intercambio de información. Deben existir acuerdos entre las partes de intercambio de información para garantizar tanto el uso que se le va a dar a la información como los niveles de protección.

13.2.3 Mensajería electrónica. El correo electrónico debe ser tratado como un activo más de información donde se apliquen controles apropiados para mantener la confidencialidad, Integridad y disponibilidad de la información.

13.2.4 Acuerdos de confidencialidad y de no divulgación. Se deben considerar acuerdos de confidencialidad tanto a personal propio como a clientes y proveedores si tiene acceso a activos de información que así lo requieran.

Almacenamiento de archivos. Controles para establecer:

A13 Seguridad en las comunicaciones.
A13.2 Intercambio de información. Requisitos o controles para proteger la información cuando se transmiten datos bien sea internamente o entre varias entidades.

13.2.1 Políticas y procedimientos de intercambio de información. Definir procedimientos y políticas para proteger la información que se va a transmitir donde se tenga en cuenta todos los aspectos.

13.2.2 Acuerdos de intercambio de información. Deben existir acuerdos entre las partes de intercambio de información para garantizar tanto el uso que se le va a dar a la información como los niveles de protección.

13.2.3 Mensajería electrónica. El correo electrónico debe ser tratado como un activo más de información donde se apliquen controles apropiados para mantener la confidencialidad, Integridad y disponibilidad de la información.

13.2.4 Acuerdos de confidencialidad y de no divulgación. Se deben considerar acuerdos de confidencialidad tanto a personal propio como a clientes y proveedores si tiene acceso a activos de información que así lo requieran.

Apache 2.4.25. Controles para establecer:

A12 Seguridad de las operaciones.

A12.1 Procedimientos operacionales y responsabilidades. Asegurar la operación correcta y segura de las instalaciones de procesamiento de información.

A12.2 Protección ante software malicioso. Garantizar que la información y las instalaciones de procesamiento de información se encuentren protegidos contra el código malicioso.

12.2.1 Controles ante software malicioso. Disponer de sistemas de detección de código malicioso en los servidores y en los puestos de trabajo.

12.3 Respaldo - copias de seguridad. Evitar la pérdida de datos mediante la aplicación de una política de copias de seguridad que permita asegurar la disponibilidad e integridad de la información ante incidentes.

12.3.1 Copias de seguridad de la información. Debe ser definido por una política de copias de seguridad o de respaldo de la información que tenga en cuenta la periodicidad con la que se hacen las copias, esto dependerá de las necesidades de recuperación de cada tipo de información.

12.5 Control de software en la producción.

12.5.1 Instalación de software en los sistemas operativos. Mantener procedimientos para cubrir las instalaciones de Software en cualquier dispositivo dentro de la organización.
12.6 Gestión de vulnerabilidad técnica.

12.6.1 Gestión de vulnerabilidades técnicas. Gestionar nuestras posibles vulnerabilidades identificando nuestras posibles debilidades técnicas.

12.6.2 Restricciones en la instalación de software. Establecer restricciones para la instalación de software por parte de los usuarios.

PHP 5.6.30. Controles por establecer:

A12 Seguridad de las operaciones.

A12.1 Procedimientos operacionales y responsabilidades. Asegurar la operación correcta y segura de las instalaciones de procesamiento de información.

12.3 Respaldo - copias de seguridad. Evitar la pérdida de datos mediante la aplicación de una política de copias de seguridad que permita asegurar la disponibilidad e integridad de la información ante incidentes.

12.3.1 Copias de seguridad de la información. Debe ser definido por una política de copias de seguridad o de respaldo de la información que tenga en cuenta la periodicidad con la que se hacen las copias, esto dependerá de las necesidades de recuperación de cada tipo de información.

12.6 Gestión de vulnerabilidad técnica.

12.6.1 Gestión de vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

MySQL 5.7.17. Controles para establecer:

A12 Seguridad de las operaciones.

A12.1 Procedimientos operacionales y responsabilidades. Asegurar la operación correcta y segura de las instalaciones de procesamiento de información.

12.3 Respaldo - copias de seguridad. Evitar la pérdida de datos mediante la aplicación de una política de copias de seguridad que permita asegurar la disponibilidad e integridad de la información ante incidentes.

12.3.1 Copias de seguridad de la información. Debe ser definido por una política de copias de seguridad o de respaldo de la información que tenga en cuenta la periodicidad con la que se hacen las copias, esto dependerá de las necesidades de recuperación de cada tipo de información.

12.6 Gestión de vulnerabilidad técnica.

12.6.1 Gestión de vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

PhpMyAdmin 4.6.6. Controles para establecer:

A12 Seguridad de las operaciones.

A12.1 Procedimientos operacionales y responsabilidades. Asegurar la operación correcta y segura de las instalaciones de procesamiento de información.

12.3 Respaldo - copias de seguridad. Evitar la pérdida de datos mediante la aplicación de una política de copias de seguridad que permita asegurar la disponibilidad e integridad de la información ante incidentes.

12.3.1 Copias de seguridad de la información. Debe ser definido por una política de copias de seguridad o de respaldo de la información que tenga en cuenta la periodicidad con la que se hacen las copias, esto dependerá de las necesidades de recuperación de cada tipo de información.

12.6 Gestión de vulnerabilidad técnica.

12.6.1 Gestión de vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

Windows 10. Controles que establecer:

A12 Seguridad de las operaciones.

A12.1 Procedimientos operacionales y responsabilidades. Asegurar la operación correcta y segura de las instalaciones de procesamiento de información.

A12.2 Protección ante software malicioso. Garantizar que la información y las instalaciones de procesamiento de información se encuentren protegidos contra el código malicioso.

12.2.1 Controles ante software malicioso. Disponer de sistemas de detección de código malicioso en los servidores y en los puestos de trabajo.

12.3 Respaldo - copias de seguridad. Evitar la pérdida de datos mediante la aplicación de una política de copias de seguridad que permita asegurar la disponibilidad e integridad de la información ante incidentes.

12.3.1 Copias de seguridad de la información. Debe ser definido por una política de copias de seguridad o de respaldo de la información que tenga en cuenta la periodicidad con la que se hacen las copias, esto dependerá de las necesidades de recuperación de cada tipo de información.

12.5 Control de software en la producción.

12.5.1 Instalación de software en los sistemas operativos. Mantener procedimientos para cubrir las instalaciones de Software en cualquier dispositivo dentro de la organización.
12.6 Gestión de vulnerabilidad técnica.

12.6.1 Gestión de vulnerabilidades técnicas. Gestionar nuestras posibles vulnerabilidades identificando nuestras posibles debilidades técnicas.

12.6.2 Restricciones en la instalación de software. Establecer restricciones para la instalación de software por parte de los usuarios.[42]

9.2 CONTROLES Y MITIGACION DE RIESGOS DE ACUERDO A LAS MEDIDAS DE ASEGURAMIENTO PARA LOS ARCHIVOS DIGITALES

Para evitar ataques se debe principalmente identificar su sensibilidad, evaluar la vulnerabilidad y revisar configuraciones, limitar las funciones, estableciendo solo las necesarias, realizar auditorías con el fin de encontrar vulnerabilidades y realizar controles y las debidas correcciones y mantener un continuo monitoreo.[43]

---

[42] SGSI. [en línea] ISO 27001: Funciones y mecanismos de salvaguarda. 27 de abril de 2017 [consultado: 4 de mayo de 2020]. Disponible en https://www.pmg-ssi.com/2015/04/iso-27001-funciones-y-mecanismos-de-salvaguarda/

[43] PRINCIPIOS BÁSICOS DE SEGURIDAD EN BASES DE DATOS. [sitio web] Johnny Villalobos Murillo. [consultado el 21 de abr. de 20] disponible en: https://revista.seguridad.unam.mx/print/2236

Los ataques a las bases de datos son muy común y en un gran porcentaje se presentan los de tipo SQL injecction , que son capaces de vulnerar la información ya sea modificándola, borrándola o incluso, tomar el control de estas poniendo en peligro las organizaciones ya que de esa información depende el óptimo funcionamiento de ellas; es por esto que se deben mantener las debidas configuraciones y prevenciones posibles para evitar los ataques maliciosos.

De esta manera es como se dispone de la seguridad de los archivos almacenados como son las copias de documentos digitales y con la adaptación una política preventiva que solo se puede alcanzar con la gestión de riesgos por medio de auditorías especializadas en seguridad informática es posible garantizar que los datos no sean vulnerados a través de los diferentes tipos de amenazas que se encuentran y ponen en peligro su existencia.

Cabe mencionar que además de los ataques cibernéticos descritos en los anteriores puntos existen otros tipos de amenazas como son los causados fenómenos naturales como como son los terremotos, lluvias torrenciales y a nivel físico como son los daños que puede sufrir la información debido al mal estado o condiciones no aptas en el lugar en donde se ubiquen los elementos contenedores de esta entre los cuales están los incendios causados intencionalmente o por accidentes y así sucesivamente.

Una vez identificados los peligros se puede tomar el control de mitigación, eliminación de amenazas potenciales estableciendo medidas según sea necesario.

Así mismo se puede tomar la mejor decisión de las empresas que ofrecen el servicio en la nube y serán contratadas; teniendo en cuenta los niveles de protección para la seguridad de la información que estas brinden en las diferentes áreas de la seguridad de un sistema informático como de definirá en los siguientes puntos.

9.3 SEGURIDAD EN PÁGINAS WEB

Esta temática es de vital importancia, puesto que hoy en día hay muchos servicios que se ofrecen vía online, por tanto, asumir estos riesgos podrían afectar los sistemas o bases de datos de una organización; el mal uso de la internet es una de las principales causas, la cual nos expone a una diversas vulnerabilidades entre las cuales vemos: Inyecciones SQL, Remotos (RFI), entre otros, que se pueden implantar a través de la visita a sitios web desconocidos o descargas e instalación de programas gratuitos atractivos de dudosa procedencia.

El objetivo de la seguridad en páginas web, es prevenir y advertir el acceso a sitios web que puedan producir robo de información o infiltración de malware a la infraestructura de las telecomunicaciones de propiedad del usuario o una

organización. Adicionalmente, hay que asegurar que los sitios web de propiedad de una organización o usuario, no sean objeto de ataques o sean vulnerados.[44]

9.4 Seguridad en Sistemas Operativos

La importancia de la seguridad en sistemas operativos se basa en los mecanismos de protección a los sistemas que administra y gestiona un usuario o una empresa, para evitar la pérdida de datos, mantener el control de la confidencialidad y controlar el acceso a los recursos.

Su objetivo es garantizar que ningún tipo de ataque informático se infiltre en los sistemas, evitando fuga de información o daños en el sistema.[45]

9.5 Criptografía

Es importante sobre todo para la gran mayoría de las organizaciones, ya que se interesa por asegurar el envío de información confidencial por un medio inseguro, mediante métodos de cifrado, en donde si se tiene acceso a esta información por entes externos o que no tengan autorización para su acceso, la información no pueda ser útil a menos que sea descifrada.

El objetivo es implementar sistemas de cifrado para garantizar al propietario de la información y su destinatario, que el contenido se emita y llegue de manera confidencial, integra y autentica.

9.6 Análisis forense

Su importancia radica en que es un proceso de análisis que se aplica en investigaciones, donde se desea encontrar algún tipo de evidencia principalmente en discos duros, sin alterar su estado, para arrojar un resultado mediante el uso de herramientas especializadas.

El objetivo es identificar, adquirir, analizar y presentar información esencial que pueda servir como evidencia en una investigación sobre delitos informáticos.

---

[44] H. FEDERICO. [en linea]. Inyección de Código: 2013 [consultado: 30 de abr. de 20]. Disponible en: https://es.slideshare.net/federicohernandezgonzalez5/inyeccion-de-codigo

[45] Marketing, «opendatasecurity,» 20 junio 2017. [consultado: 30 de abr. 20]. Available: https://opendatasecurity.io/es/5-ciberataques-mas-importantes-en-lo-que-llevamos-2017/.

9.7 RIESGO Y CONTROL INFORMÁTICO

La importancia de conocer los riesgos y controles informáticos se basa en ayudarnos a conocer las vulnerabilidades a las cuales nos enfrentamos y aplicar medidas de seguridad que conlleven a prevenir ataques informáticos a nuestra empresa.

El objetivo es prevenir ataques informáticos, reconociendo los riesgos y los controles para prevenirlos.

9.8 CRONOGRAMA

Para la seguridad de la información es necesaria la elaboración de estrategias que definan el tiempo para el cumplimiento del plan de la realización de las copias cuando es en gran volumen.

Esto se lleva a cabo estableciendo un periodo de tiempo dentro del cual se realicen reportes del cumplimiento, además se deben reportar anualmente los informes del programa establecido con dichos reportes del plan de conservación documental.

- DIRECTOR

Quien realice o dirija las medidas del plan debe ser un profesional de bibliotecología e informática.

- RECURSOS

Proveer los medios necesarios para lograr el objetivo de mantener a salvo la documentación importante

- RESPONSABILIDAD

Es compromiso de cada entidad prestadora de servicios ofrecer los recursos tanto económicos como tecnológicos para llevar a cabo el cumplimiento de las actividades.

9.9 ESTRATEGIAS PARA LLEVAR EL PROCESO DE LA SEGURIDAD INFORMATICA ENFOCADA EN LA PRESERVACION DE DOCUMENTOS DIGITALES

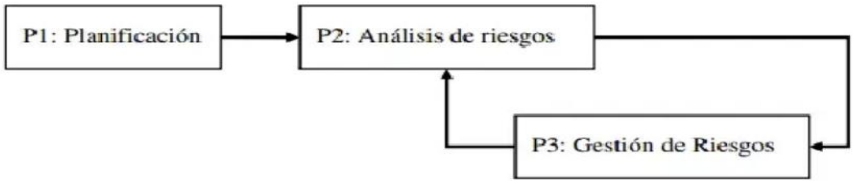
Con el fin de realizar un proceso de seguridad informática bien aplicado teniendo en cuenta los diferentes elementos que conforman la información y sin dejar de lado las leyes como son las estipuladas según el artículo 5 del ACUERDO 004 DE 2019 (el cual se explicará detalladamente más adelante) y además establecer políticas que técnicamente se encuentren dentro de la normativa como son las metodologías que se rigen por estándares internacionales, utilizadas para analizar los riesgos y amenazas a los que puede estar expuesta ésta en las diferentes entidades y que son utilizadas por expertos en seguridad informática; cabe mencionar que a pesar de que son diferentes las entidades, estas giran en torno mismo propósito o modelo de sistema en cuanto a información se refiere y a la vez se pueden complementar con modelos de referencia incorporando técnicas y normas estándares de seguridad internacional como ya se ha mencionado.

Entre las muchas metodologías usadas para análisis y gestión de riesgos se mencionan a continuación.

9.9.1 MAGERIT

[46]Esta metodología es de carácter público y se compone de tres libros (métodos, catálogo de elementos y guías técnicas) los cuales proporcionan el paso a paso para cumplir con eficiencia el proceso completo del análisis de riesgos en organizaciones. En la siguiente imagen se muestras sus fases.

Figura 19. Fases del Análisis de riesgo con Magerit



Fuente: Portal de Administración Electrónica. Ministerio de Asuntos Económicos y Transformación Digital · Secretaría General de Administración Digital. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[46] © Portal de Administración Electrónica [en linea]· Ministerio de Asuntos Económicos y Transformación Digital · Secretaría General de Administración Digital. [consultado el 5 de abril de 20211]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

El modelo para seguir según esta metodología es el siguiente:

9.9.2 DETERMINAR LOS ACTIVOS

Considerados como los bienes tangibles e intangibles de la organización y se clasifican en:

[S] Servicios
[D] Datos
[SW] Aplicaciones
[HW] Equipos informáticos
[COM] Redes de comunicaciones
[SI] Soportes de información
[AUX] Equipamiento auxiliar
[L] Instalaciones y personal
[P] personal

En este paso se determinan las amenazas a las que se encuentran expuesto los activos
Se estipulan las medidas de control y salvaguardas sobre los activos en riesgo
Se evalúa el impacto producido en caso de que se materialice la amenaza
Se mide el riesgo referido a la materialización de la amenaza

9.9.3 OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET AND VULNERABILITY EVALUATION)

Utilizada para recolectar información que pueda ser de gran ayuda para eliminar o mitigar los riesgos y amenazas a nivel operacional dentro de las organizaciones

9.9.3 ISO 27001:2013

Su principal propósito es encontrar las vulnerabilidades y establecer controles de seguridad

Figura 20. Estructura ISO

Fuente: Estructura ISO 27001. [consultado: 16 de noviembre de 2020] disponible en https://advisera.com/wp-content/uploads/sites/5/2014/05/Estructura-de-ISO27001.png

ANEXO A SOBRE LOS CONTROLES DE SEGURIDAD EN ISO 27001

[47]"Los controles de seguridad en ISO 27001 son 114. Distribuidos dentro del Anexo **en 14 secciones**, así:
Políticas de seguridad de la información: A. 5.
Organización de la seguridad de la información: A.6.
Seguridad de los recursos humanos: A. 7.
Gestión de Activos: A.8.
Controles de acceso: A.9.
Criptografía – Cifrado y gestión de claves: A.10.
Seguridad física y ambiental: A.11.
Seguridad operacional: A.12.
Seguridad de las comunicaciones: A.13.
Adquisición, desarrollo y mantenimiento del sistema: A.14.
Gestión de incidentes de seguridad de la información A.16.
Cumplimiento: A.18"

[47] Escuela Europea de Excelencia Artículos Tecnicos, Destacado, Seguridad y Salud en el Trabajo. [sitio web]. El Anexo A y los controles de seguridad en ISO 27001: consultado en: https://www.escuelaeuropeaexcelencia.com/2019/05/el-anexo-a-y-los-controles-de-seguridad-en-iso-27001/

10 BENEFICIOS DE CONTAR CON EL RESPALDO DE LA DOCUMENTACIÓN DIGITAL

Frente al gran número de amenazas que día a día se presentan y que ya se han expuesto anteriormente como son los desastres naturales, accesos no autorizados en el área física en donde se encuentran los archivos o documentos y la ciberdelincuencia, es necesario emplear mecanismos que permitan la protección de la información y escoger la mejor de las opciones con el fin de garantizar prestigio de las organizaciones ya que la información en éstas, es uno de los activos más valiosos, por lo que la implementación de estrategias de recuperación de desastres como son las copias de seguridad es de gran ayuda para la tranquilidad y permanencia tanto de negocios así como de entidades gubernamentales entre otros.

De lo contrario, los riesgos materializados pueden ser tan graves que llevarían a dichas entidades a millonarias pérdidas financieras como fue el caso Saudi Aramco en donde muchos cibercriminales ubicados en Rumanía accedieron de forma fraudulenta a los sistemas electrónicos del gigante saudí y como consecuencia de esto, la petrolífera tuvo millones de dólares en pérdidas e innumerables daños materiales. (Redacción APD,2018)

10.1 PLAN ESTRATEGICO DE CONSERVACION DE DOCUMENTOS DIGITALES EN DIFERENTES MEDIOS DE ALMACENAMIENTO

Conociendo la estructura de las anteriores metodologías descritas y sus respectivos controles en sistemas informáticos, se establece un plan estratégico para la conservación de documentos digitales.

Si bien la información almacenada en soportes como copias en papel, como es el caso de las empresas donde se requiere constancias de firmas entre otros, es importante establecer medidas de respaldo de dicha documentación debido al alto riesgo que el soporte de almacenamiento mencionado; en consecuencia de esto, las copias deben ser recopiladas no solo en papel sino que se deben utilizar diferentes métodos de aseguramiento y respaldo donde la información se encuentre segura según las normas establecidas para lograrlo correctamente.

Dado el ejemplo anterior de amenazas y controles por medio de la metodología MAGERIT y la ISO 2101: 2013 se aplicarían las medidas de contingencia necesarias en cualquier tipo de organización requeridas por los estándares obligatorios pero, además de eso se aplican los controles de seguridad “Seguridad física y ambiental: A.11” al área de documentos y archivos dando respaldo con copias digitales en diferentes medios de almacenamiento, para el caso de las empresas donde se maneja información sensible es necesario crear copias en diferentes medios como

son los **cd**, memorias **USB** y **discos extraíbles** teniendo en cuenta el lugar donde serán guardados de modo que el lugar no sea dentro de la empresa.
Otro aspecto importante es el control de “Criptografía – Cifrado y gestión de claves: A.10.” donde la información almacenada en los diferentes soportes digitales debe estar protegida con claves secretas seguras y la información debe estar encriptada estableciendo así el control de acceso.
Establecidas estas políticas de seguridad se hace necesario ir más allá en el sentido de facilitar el acceso a usuarios autorizados aprovechando el uso de las tecnologías en la red como son las backups.

10.1.1 ESTRATEGIAS DE CREACIÓN DE BACKUPS

Una vez analizados todos los posibles riesgos en los sistemas informáticos empresariales, es de contemplar como medidas de control y mitigación de riesgos el establecer en las políticas de seguridad más recursos que garanticen la disponibilidad de la información permitiendo el acceso remoto a personas autorizadas, obtener copias sin modificar o manipular las copias originales, entre muchos otros aspectos que permiten un alto grado de tranquilidad en cuanto a la seguridad y permanencia de tales documentos.

Existen tres modos fundamentales de realizar las copias de seguridad en las empresas y esto depende tanto de la forma en que estas llevan sus procesos de almacenamiento de datos y del plan escogido ofrecido por las empresas para tal fin. Estas formas son: incremental, diferencial y seguridad completa.

Copias de seguridad incremental

Este tipo de copias se van realizando día a día sin realizar cambios a las anteriormente guardadas.

Copias de seguridad diferencial

Este tipo de copias se van realizando de forma completa cada día y va guardando los cambios.

Copias de seguridad completa

Seguridad de información de bases de datos internas

Estas se deben llevar separadas del sistema con el fin de proteger los datos importantes de las organizaciones.

Almacenamiento fuera de las instalaciones

Debido a las crecientes amenazas de robo de información también llamada ransomware, así como desastres naturales, se hace necesario llevar extremadas medidas de precaución como es realizar un tipo de almacenamiento que se pueda mantener fuera de las oficinas y sitios de trabajo con el fin de protegerles; la información debe estar guardada en discos externos en sitios claves y confidenciales y para mayor seguridad, en la nube.

Almacenamiento en línea

Este tipo de copias son llevadas por conexión segura en la nube y se puede acceder en cualquier momento a la información por usuarios autorizados. Este lo proveen los servicios Cloud.

Copias de seguridad espejo

Las copias de seguridad en este modo son una fiel copia de lo almacenado en las estaciones de trabajo de modo que si se borra un archivo el que se encuentra en la copia también se borra; esto implica tener mucho cuidado en las manipulaciones de dichos documentos.

10.2 PRINCIPIOS DE LA PRESERVACION DIGITAL

Para establecer la autenticidad de los documentos electrónicos digitales es La Agencia Nacional para la Defensa Jurídica del Estado quien se encarga de la respectiva revisión, en función a esto el documento almacenado debe contar con algunos requisitos lógicos de estructura sin importar el medio donde será conservado y el formato que posea, pero identificando el funcionamiento del proceso del manejo de la información como son las siguientes características de recepción de esta en las organizaciones.

El flujo: se identifica tanto el control como la generación de documentos en las entidades.

Canal: son las diferentes formas de como se recibe y almacena la información, dependiendo de la actividad la información puede ser recibida manualmente y soportada en papel o electrónicamente.

Conversión: según las políticas y necesidades se realiza la conversión a medios electrónicos digitales en formatos requeridos.

Reemplazo: se define si las copias digitales de los documentos pasan a ser definitivas reemplazando los medios físicos de soportes utilizados en primera instancia al recibir la información.

Formato: según la necesidad de la organización o entidad se definen los tipos de extensión que tendrán los ficheros.

Metadatos: es el conjunto de documentos que se obtienen de entrada y deben ser identificados para su destino de almacenamiento y preservarlos estableciendo su ruta e identificar cada componente por medio del cual identificarle y acceder posteriormente a su contenido.

Dentro del plan de preservación documental digital es necesario incluir procesos de **digitalización certificada**, de acuerdo con el Protocolo de Digitalización con Fines Probatorios, expedido por el
Archivo General de la Nación y la Guía No. 5 Y el acuerdo 27 de 2016 del concejo del archivo de la nación[48] entre otros apartados ya mencionados anteriormente por medio de los cuales se establece la digitalización y la autenticidad de los documentos.

Otro aspecto importante son las **versiones** si los documentos son cambiantes y de forma incremental como es el caso de las historias clínicas o solicitudes en donde se generan nuevos datos que se deben adicionar a los expedientes de usuarios estos deben ir estipulados por versiones según su modificación.

Teniendo en cuenta que las copias digitales deben permanecer a largo plazo se consideran las formas de almacenamiento sin dejar de lado los protocolos y requerimientos de seguridad de la información con sus controles de recuperación y continuidad de los metadatos procesados y generado, sino que se estableces medidas de fácil acceso y comodidad para los usuarios llegando nuevamente al tema de las backups como una de las opciones seguras y viables dentro de los planes de recuperación y acceso inmediato a los archivos y copias digitales resguardadas.

[48]Colombia. Archivo General de la Nación. Protocolo para Digitalización de Documentos con Fines Probatorios. Comité de Reprografía
y Automatización del Sistema Nacional de Archivos. Bogotá, 2011.

11 ANALISIS DE LOS RESULTADOS DEL PROYECTO

Mediante las metodologías que se describen anteriormente se logra identificar los tipos de riesgos y amenazas que pueden afectar un sistema de información ya sea en una empresa o cualquier otro tipo de entidad; para el caso de un conjunto de archivos y/o documentos es posible que éstas tomen medidas de aseguramiento y establezcan políticas de control utilizando los recursos tecnológicos disponibles que pueden ser a muy bajo costo el cual puede incrementar dependiendo de la necesidad de protección y de los planes ofrecidos por distintas empresas que ofrecen el servicio de almacenamiento y respaldo de la información según en volumen requerido.

Dependiendo la dimensión de la empresa o entidad se puede combinar las metodologías y técnicas como por ejemplo en el caso de resguardo de archivos y documentos digitales es posible realizar una auditoría con Magerit y aplicar los controles del anexo A de la ISO 2701:2013 aclarando que solo se aplican los necesarios para el cumplimiento de la seguridad de la información según el tipo de entidad en este caso se aplicarían los siguientes:

Políticas de seguridad de la información: A. 5.
Controles de acceso: A.9.
Criptografía – Cifrado y gestión de claves: A.10.

Para el aseguramiento en la nube se procede a contratar servicios de respaldo y almacenamiento; como ejemplo se muestra la empresa "**Digitalización y resguardo de archivos**" cuya misión se describe de la siguiente manera [49]"Digitalización y Resguardo de Archivos S de RL de CV es una empresa joven que ha visualizado hacia el futuro mediato e inmediato lograr ser una organización líder en la digitalización de archivos documentales, para las empresas micro, pequeñas y medianas, locales, regionales, nacionales e internacionales"

Donde afirma que uno de los [50]motivos para resguardar los archivos no solo son por seguridad sino que la ley obliga a todas las empresas a guardar todos sus comprobantes fiscales de por lo menos 5 años, lo que generaría gran cantidad de volumen en papelería y que esto facilitaría la disponibilidad de documentos en cualquier eventualidad, evitando el desperdicio de espacio útil almacenando documentos de uso poco frecuente, el extravío de documentos que pueden traer problemas legales, fiscales, baja productividad o mal servicio con sus clientes por no encontrar oportunamente documentos importantes, el desperdicio del tiempo de personal para encontrar documentos y algo muy importante que es evitar que personas no autorizadas tengan acceso a información delicada o confidencial para el caso de negocios o empresas.

---

[49]. DIGITALIZACIONYRESGUARDO. [en línea]. TODOS LOS DERECHOS RESERVADOS. COPYRIGHT (C) 2013 Disponible en: http://www.digitalizacionyresguardo.com/quienessomos.html

[50] http://www.digitalizacionyresguardo.com/resguardo.html

Desde otro punto de vista se analizan los procedimientos que deben seguir las organizaciones gubernamentales, como lo expresado en el blog "la voz del bibliotecario" en su publicación titulada **Administración y preservación de archivos digitales,** afirmando lo siguiente:

[51]"Artículo 6to constitucional Fracción V, dice: Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos"

Refiriéndose según La Ley Federal de Archivos en México, no obstante en Colombia también se decretan leyes similares que obligan a los gobiernos establecer una serie de requisitos para un proceso en el que se identifiquen y se organicen técnicamente los documentos de archivos producidos por dicha entidad, los cuales se encuentran estipulados meticulosamente desde el artículo 1 hasta el artículo 5 del ACUERDO 004 DE 2019 [52]"Por el cual se reglamenta el procedimiento para la elaboración, aprobación, evaluación y convalidación, implementación, publicación e inscripción en el Registro único de Series Documentales – RUSD de las Tablas de Retención Documental – TRD y Tablas de Valoración Documental – TVD

EL CONSEJO DIRECTIVO DEL ARCHIVO GENERAL DE LA NACIÓN JORGE PALACIOS PRECIADO

En ejercicio de sus facultades legales, en especial las que le confiere la Ley 80 de 1989, el artículo 76, literal b) de la Ley 489 de 1998, la Ley 1470 de 2011, el Decreto 2126 de 2012, el Decreto 1080 de 2015, el Acuerdo 09 de 2012 en conformidad al artículo 2.2.22.3.8 del Decreto 1499 del 11 de septiembre de 2017, establece que en cada una de las entidades del orden nacional o territorial se debe integrar un "Comité Institucional de Gestión y Desempeño" encargado de orientar la implementación y operación del Modelo Integrado de Planeación y Gestión – MIPG, dentro del cual se incluye la política de Gestión Documental" [AGN]

De esta manera se puede decir, que además de los beneficios que se obtienen estableciendo y adoptando las medidas de seguridad de los archivos en forma digital, es un compromiso de las empresas y entidades de los gobiernos contar con un respaldo de digitalización de sus documentos.

De acuerdo con anterior análisis, es preciso optar para la solución de la problemática inicial en cuestión, llevar un plan estratégico para gestionar un sistema de control de riesgos para evitar la pérdida de información en las empresas o entidades ya sea públicas o privadas en el que se establezcan políticas que procedan a la creación de copias digitales y adoptar planes de servicios de almacenamiento que se ajusten a la necesidad de los procesos y volúmenes de

---

[51] Administración y preservación de archivos digitales
Por. F. Terrazas. [sitio web]. Unidad de ServiciosBibliotecarios.Coordinación General del SUBA, disponible en: https://fterrazas.wordpress.com/divulgacion-bibliotecaria-2/administracion-y-preservacion-de-archivos-digitales/

[52] Archivo General de la Nación. Todos los derechos. [sitio web] © Derechos reservados 2018. Disponible en: https://normativa.archivogeneral.gov.co/acuerdo-004-de-2019/

información generados en ellas; entre de los controles que facilitan dichos procesos y de acuerdo a las normas que regulan las buenas prácticas en la seguridad de sistemas de información las copias digitales son esencialmente importantes, las políticas deben establecerse en las respectivas áreas dentro de las empresas, priorizar y escoger el tipo de información a guardar y las estrategias a utilizar, en lo que se puede elegir:

Realizar copias digitales en medios magnéticos, memorias USB o discos duros externos y además sean llevados fuera de la empresa bajo la responsabilidad de un ente de la empresa o entidad correspondiente.

Se pueden realizar copias en la nube ya sea de forma incremental, parcial o completa; esto se logra contratando un servicio de preservación digital, cuyo valor es según la capacidad de almacenamiento en la gestión de documentos empresariales. A continuación, se mencionan algunas empresas proveedoras del servicio de copias en la nube:

- Odilo preserver[53], quien ofrece diferentes soluciones en el campo informático entre ellos el Servicio de preservación 100% OAIS (Open Archival Information System).

- DONGEE, permite un control total de la programación de las copias de respaldo y niveles de encriptación más altos que protegen la información frente a robo, malware o ransomware[54].

- Dropbox, para migrar datos de diferentes plataformas o sistemas operativos.

- Google Drive/ Google One, que es el más común hoy día, utilizado en diferentes dispositivos como celulares y pc.

Así mismo, existen muchas más compañías proveedoras de este tipo de servicios que solo queda escoger según las políticas y conforme a la calidad y capacidad requerida por el cliente y el tiempo que sea necesario en la conservación de la información.

---

[53] ODILO. Odilo preserver. [en linea]. [consultado el 26 de marzo de 2021] disponible en: https://www.odilo.es/preservacion/?gclid=EAIaIQobChMIvuTLhoPO7wIVreiGCh3gJQCiEAAYASAAEgLr9vD_BwE

Dongee. Acronis Backup Server [en linea]. [consultado 26 de marzo de 2021] disponible en: https://www.dongee.com/hosting/cloud/colombia/?utm_source=google&utm_medium=cpc-keyword&utm_campaign=vps&as_clid=a64c4acf-23a9-476c-8a57-92f2ba4f983b:servidores%20de%20almacenamiento%20en%20la%20nube:e:g:&gclid=EAIaIQobChMI3oebso3O7wIVEW-GCh3LvQBmEAAYAiAAEgIckPD_BwE

[54]

CONCLUSIONES

-Se analizaron las diferentes formas en que se pueden crear copias digitales de documentación para asegurar su disponibilidad y la preservación, encontrándose alternativas muy viables que satisfacen la necesidad de las entidades de acuerdo a lo que cada una de estas requiera, basándose en la naturaleza y el tipo de documento a preservar y en el volumen que se genere en un periodo de tiempo.

-Entre las diferentes tecnologías utilizadas para mantener copias de seguridad se pueden identificar diferentes tipos de mecanismos y medios posibles, considerando como el más opcional según sus ventajas las backups.

- Mediante el respaldo de la documentación digital por medio de backups o el medio de almacenamiento elegido por las organizaciones o entidades privadas o particulares se puede decir que es muy importante ya que según la necesidad se pueden conservar documentos o diferentes tipos de archivos según la tecnología seleccionada, esto es, tipo incremental, diferencial u otro modo más conveniente, pudiendo contar con dicha información en cualquier momento sin importar que tanto tiempo pase.

-Las medidas de seguridad de la información son importantes ya que previenen desastres o perdida de información valiosa tanto tipo histórica como para información empresarial, tales medidas se pueden tomar según el riesgo en que se encuentre la información a proteger y por medio de diferentes metodologías que existen para dicho fin. Una de las mejores estrategias es implementar políticas de seguridad que conlleve a crear copias de respaldo y mantenerla fuera de los lugares físicos de trabajo ya sea los sitios físicos o en servidores remotos.

-Las metodologías utilizadas para la identificación de amenazas y riesgos que exponen a la información y datos almacenados son de gran importancia ya que por medio de los errores y falencias que se encuentren en las entidades se pueden tomar las medidas de precaución y hasta mitigar o eliminar los llamados huecos tanto a nivel físico como lógico en las plataformas informáticas; de ahí que los medios de almacenamiento se encuentren a salvo en caso de materialización de eventos desastrosos provenientes de cualquier fenómeno natural o intencional como es la ciberdelincuencia entre otros.

REFERENCIAS

- Acens Technologies. Bases de datos y sus vulnerabilidades más comunes. [sitio web] Acens.com 2015, 3 de marzo. [consultado 21 de abr. de 20]. Disponible en: https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf
- Actividades para la ejecución del plan. Sistema integrado de conservación. [en línea] Mintic.gov.co 2020. [consultado 21 de abril de 2020] https://www.mintic.gov.co/portal/604/articles-7077_sistema_integrado_conservacion_v20180507.docx
- Administración y preservación de archivos digitales Por. F. Terrazas. Unidad de Servicios Bibliotecarios. [en línea]. Coordinación General del SUBA: 2016, 28 de octubre. [consultado el 21 de abril 2020] disponible en: https://fterrazas.wordpress.com/divulgacion-bibliotecaria-2/administracion-y-preservacion-de-archivos-digitales/
- ALBA CABAÑAS, Marisleidy, VALENCIA BONILLA, María Beatriz y MEJÍA RAMÍREZ, Melba Lida. Los Sistemas de Información de Marketing en las organizaciones actuales: La utilización de herramientas para la toma de decisiones. Scientia et Technica [en línea] ISSN 0122-1701, Vol. 19, n. 1, 2014, p. 54-58. [Consulta 23-9-2015]. Disponible en: http://www.redalyc.org/articulo.oa?id=84930900009
- Archivo General de la Nación Colombia. [sitio web]. ACUERDO 006 DE 2014. 15 abril, 2014. [consultado 19 de abr. de 20] disponible en: https://normativa.archivogeneral.gov.co/acuerdo-006-de-2014/
- Archivo General de la Nación. [sitio web]. Normativa 2018. Disponible en: https://normativa.archivogeneral.gov.co/acuerdo-004-de-2019/
- ARTILES, Visbaly Sara M. La gestión documental, de información y el conocimiento en la empresa. [en línea]. El caso de Cuba: 2009. ACIMED, ISSN 1024-9435. [Consulta 23-9-2015]. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S10249435200900050002
- BAENA, PAZ, Guillermina María Eugenia. Metodología de la investigación 2014, Grupo Editorial Patria. ProQuest Ebook Central. [en línea] pag.74–82. [consultado: diciembre de 2020] Recuperado de: https://bibliotecavirtual.unad.edu.co:2538/lib/unadsp/detail.action?docID=3228423.
- BLANCO, Ana del Arco Y ROJAS SOSA, Luna. El archivo de Internet: depósito legal de las publicaciones electrónicas tras el Real Decreto 635/2015, de 10 de junio. [en línea]. Granada: Comares, 2016. [Consulta 04-03- 2019]. https://dialnet.unirioja.es/servlet/libro?codigo=655559

- Blog de la biblioteca de Traducción y Documentación de la Universidad de Salamanca. [sitio web]. Universoabierto.org 2018. [consultado el 24 de marzo de 2021]. Disponible en: https://universoabierto.org/2018/01/18/65libros-gratis-e-informes-sobrearchivos-y-archivistica/ (2017).
- Blog especializado en Sistemas de Gestión de Seguridad de la Información: Algunos ejemplos de incidentes de seguridad de la información, 2017ISO 27001:2013. [en línea]. Pmg-ssi.com 2017, 16 de febrero. [consultado: 30 de abr. de 20]. Disponible en: https://www.pmg-ssi.com/2017/02/algunos-ejemplos-de-incidentes-de-seguridad-de-la-informacion/
- BORDA PÉREZ, M. [sitio web]. El proceso de investigación: visión general de su desarrollo. (pag.80-89). Barranquilla, Colombia: Universidad del Norte Search.ebscohost.com 2013. [Consultado el 20 de agosto de 2020] Recuperado de http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=710213&lang=es&site=eds-live&scope=site.
- CANDAS ROMERO, Jorge. [sitio web]. El papel de los metadatos en la preservación digital. El profesional de la información 2006, ISSN 1386-6710, Vol. 15, n. 2, 2006, p. 126-136. [Consulta 04-03-2019]. Disponible en: http://eprints.rclis.org/8359/1/final.pdf
- Centro de Conversión de Documentos e Imágenes, S.A. de C.V. (Imaging Center): Origen y concepto de Digitalización. [en línea] El equipo de marketing Digitalización 2011. [consultado: el 18 de abr. de 20] disponible en: http://www.imaging.mx/origen-y-concepto-de-digitalizacion/
- Centro de innovación. [sitio web] Cero papeles en la administración pública. Mintic: 2021, 22 de marzo. [consultado el 23 de marzo de 2021]. Disponible en: https://centrodeinnovacion.mintic.gov.co/es/sobre-el-centro/que-es
- Ciberataques. [sitio web]. Opendatasecurity : 2017, 20 de junio. [consultado: 30 de abr. 20]. Available: https://opendatasecurity.io/es/5-ciberataques-mas-importantes-en-lo-que-llevamos-2017/.
- Configuración de Mecanismos de Seguridad. [en línea].Tipos de amenazas físicas U8. Virtual.itca.edu.sv. [consultado el 2 de mayo de 20]. https://virtual.itca.edu.sv/Mediadores/cms/u48_tipos_de_amenazas_fsicas.html
- Definición.de [sitio web] [Consultado: 27 de abr. De 20]]disponible en: https://definicion.de/digital/ Consultado en : https://www.google.com/search?q=formato&oq=formato&aqs=chrome..69i57j35i39l2j0l5.3764j0j7&sourceid=chrome&ie=UTF-8
- Dongee. [sitio web]. Acronis Backup Server [consultado 26 de marzo de 2021] disponible en: https://www.dongee.com/hosting/cloud/colombia/?utm_source=google&utm_medium=cpc-keyword&utm_campaign=vps&as_clid=a64c4acf-23a9-476c-8a57-92f2ba4f983b:servidores%20de%20almacenamiento%20en%20la%20nube

:e:g:&gclid=EAIaIQobChMI3oebso3O7wIVEW-GCh3LvQBmEAAYAiAAEgIckPD_BwE

- Escuela Europea de Excelencia Artículos Técnicos, Destacado, Seguridad y Salud en el Trabajo. [en línea] 2020, 7 de mayo. El Anexo A y los controles de seguridad: ISO 27001 [consultado 23 de marzo de 2021] disponible en: https://www.escuelaeuropeaexcelencia.com/2019/05/el-anexo-a-y-los-controles-de-seguridad-en-iso-27001/
- GARCÍA DE CELIS, Ciriaco. [en línea]. «El disco duro del AT (IDE, MFM, BUS LOCAL).». (4ª edición). Facultad de Ciencias de Valladolid 1994: Grupo Universitario de Informática.
- GESTIÓN DEL REPOSITORIO DOCUMENTAL DE LA UNIVERSIDAD DE SALAMANCA. [en línea]. Educación y biblioteca, Año 9, n. 80, p. 28-41 disponoble en: gredos.usal.es/jspui/handle/10366/113397
- Gestión Documental. [en línea]. Tic.portal.es: 2017. [consultado el 23 de marzo de 2021] disponible en: ticportal.es/temas/sistemagestion-documental/digitalizacion-dedocumentos
- GONZÁLES CAM, Celso. Convención Nacional de Centros Binacionales – Trujillo [en línea]. Perú: 2007, octubre 11. [consultado el 23 de marzo de 2021] disponible en: archivisticayarchivos.files.wordpress.com/2012/11/la_importancia_de_la_digitalizacic3b3n_de_archivos_para_la_bie280a6
- H. FEDERICO. [sitio web]. Inyección de código: 2013. [consultado: 30 de abr. de 20]. Disponible en:
- ICA.ORG. [en línea] International Council on Archives 2016. [Consultado: 30 de abr. De 20] Disponible en: https://www.ica.org/es/%C2%BFqu%C3%A9-son-los-archivos
- III Plan Estratégico 2019-2023 - Consejo de Cooperación Bibliotecaria. www.ccbiblio.es/wp-content/uploads/III-Plan-Estratégico-CCB-def.pdf
- INCIBE. [sitio web] Análisis de riesgos en 6 pasos Seguridad y auditoria de sistemas: 2017, 1 de junio. [consultado: 4 de mayo de 2020] Disponible en: https://www.incibe.es/en/node/2789
- Institución de Educación Superior sujeta a inspección y vigilancia por el Ministerio de Educación Nacional. [en línea]. Personería jurídica Res. 192 de 1946-06-27 – Ministerio de Gobierno. Unilibre: 2016, 16 de marzo. [consultado: 7 de abr. De 20] disponible en: https://www.mintrabajo.gov.co/documents/20147/58606751/VALLE+DEL+CAUCA+AFL+UNIVERSIDAD+LIBRE+SUSCRITO.pdf
- Instituto internacional de investigación y desarrollo tecnológico educativo INDTEC. [en línea] Revista scientific volumen 4, num.14 Revista Arbitrada Multidisciplinaria de Investigación Socio Educativa Volumen 4, N.º 14.2019-2020/ Venezuela/ Edición Trimestral: Indteca.com 2019-2020. [consultado 5 de abr. de 2020] disponible en: http://www.indteca.com/ojs/index.php/Revista_Scientific/issue/view/28/Scientific.issn.2542-2987.2019.4.14

- Investigación bibliotecológica [versión On-line] ISSN 2448-8321.Versión impresa ISSN 0187-358X Investig. bibl vol.24 no.50 México. Artículos Preservación documental digital y seguridad informática [consultado: 19 de abr. de 20] disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008#nota
- Ley Estatutaria 1581 de 2012 - Secretaría del Senado. [en línea] Diario Oficial No. 48.587 de 18 de octubre de 2012 CONGRESO DE LA REPÚBLICA. [consultado: el 19 de mayo de 2020] disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
- Library.umass.edu. Banach, M. [e-Book] 2011. Guidelines ***for Digitization***, Massachusetts: University of Massachusetts, UMass Amherst Libraries. Digital Creation and Preservation Working Group,. [Consultado 23 de marzo 2021] disponible en: https://www.library.umass.edu/assets/Digital-Strategies-Group/Guidelines-Policies/UMass-Amherst-Libraries-Best-Practice-Guidelines-for-Digitization-20110523-templated.pdf
- MAGERIT v.3. [en línea] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [consultado: 5 de mayo de 2020] disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
- MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE, [sitio web] Bibliografía: El Repositorio Institucional. Identificación, Almacenamiento. 2015, 27 de abril. [Consultado el 3 de sep. 2020] disponible en: http://www.bne.es/webdocs/Inicio/Perfiles/Bibliotecarios/bibliografia-oposiciones/25._Bibliografxax_El_repositorio_institucional._Identificacixn...pdf
- MIQUEL RAFFINO, María Estela. [en línea]. Términs Barcelona, Editorial UOC 2013. El profesional de la información 16. 109 pp. ISBN 978-84-9029-819-0. Base de datos [consultado:5 de abr. De 20] Disponible en: https://concepto.de/base-de-datos/. [Consultado: 21 de abril de 2020]. Fuente: https://concepto.de/base-de-datos/#ixzz6KFslhFDw
- MORO CABERO, Manuela. Identificación, caracterización y selección de formatos para la preservación del recurso digital. [en línea] MÉI: Métodos de Información, ISSN-e 2173-1241, Vol. 9, n. 16, 2018, p. 49-90.2. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6528627
- MOULAISON SANDY, Heather y Edward M. CORRADO. [en línea]. Bringing content into the picture: proposing a tri-partite model for digital preservation. Journal of library administration, ISSN 1540-3564, Vol. 58, n. 1, 2018, p. 1-17 [Consultado el 21 de abril de 2020] Disponible en: http://blog.bne.es/biblioteconomia/2018/03/07/bringingcontentpictureproposing-tri-partite-model-digital-preservation/
- MURILLO, Johnny. [en línea]. PRINCIPIOS BÁSICOS DE SEGURIDAD EN BASES DE DATOS. Revista.seguridad.unam.mx. [consultado el 21 de abr. de 20] disponible en: https://revista.seguridad.unam.mx/print/2236

- NoSQL vs SQL. [sitio web]. Principales diferencias y cuándo elegir cada una de ellas. blog.pandorafms.org: 2015, 18 de noviembre. [consultado 21 de abr. de 20]. Disponible en: https://blog.pandorafms.org/es/nosql-vs-sql-diferencias-y-cuando-elegir-cada-una/
- Odilo preserver. [en línea] [consultado el 26 de marzo de 2021] disponible en: https://www.odilo.es/preservacion/?gclid=EAIaIQobChMIvuTLhoPO7wIVreiGCh3gJQCiEAAYASAAEgLr9vD_BwE
- Open Document Management System S.L. [en línea]. Conservación de documentos electrónicos. openkm.com: 2020. [consultado: 5 de abr. De 20] disponible en: https://www.openkm.com/es/blog/conservacion-de-documentos-electronicos.html Biblioteca de Catalunya. Carrer de l'Hospital, 56. 08001 Barcelona. [consultado:5 de abr. De 20] disponible en: https://www.bnc.cat/esl/Profesionales/Preservacion-digital2
- ORERA ORERA, Luisa. [en línea] Preservación digital y bibliotecas: un nuevo escenario. Revista general de información y documentación, Vol. 18, 2008, p. 9-24. [Consultado el 21 de abril 2020]. http://revistas.ucm.es/index.php/RGID/issue/view/RGID080811/showToc
- Portal de Administración Electrónica. [sitio web]. Ministerio de Asuntos Económicos y Transformación Digital · Secretaría General de Administración Digital. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
- Preservación del patrimonio documental digital en el mundo. [En línea]. Scielo.org.mx: 2007. [consultado el 24 de marzo de 2021]. Disponible en: http//:www. /scielo.php?script=sci_arttext&pid=S0187
- PRESERVACIÓN Y CONSERVACIÓN DE DOCUMENTOS DIGITALES. [sitio web] [consultado el 24 de marzo de 2021]. Disponible en: https://www.acal.es/index.php/archivposta.../95_cb791e918e1298221b2e8cfb89af233b
- Principales amenazas de un sistema informático. [sitio web]. Prakmatic.com: 2017. [consultado 2 de may. de 20]. Disponible en: http://www.prakmatic.com/uncategorized/principales-amenazas-de-un-sistema-informatico/
- PUBLICACIONES SEMANA S.A. [en línea] Así se están muriendo algunos archivos en Colombia: PATRIMONIO.Semana.com: 2016, 7 de agosto. [consultado 5 de 04 de 2020] disponible en: https://www.semana.com/cultura/articulo/documentos-en-riesgo-con-valiosa-informacion-historica/481149
- PUBLICACIONES SEMANA S.A. Ibíd. [consultado El 20 de abril de 2020] disponible en: https://www.semana.com/cultura/articulo/documentos-en-riesgo-con-valiosa-informacion-historica/481149
- Real Academia Española. [en línea]. [Consultado:30 de abr. de 20]. disponible en: https://dle.rae.es/preservar

- Red Hat Enterprise. Linux 4 Manual de seguridad. Red Hat, Inc. [en línea]. Web.mit.edu: 2015. [consultado: 2 de may. de 20]. disponible en: http://web.mit.edu/rhel-doc/4/RH-DOCS/pdf/rhel-sg-es.pdf
- RUBEN, Ramiro. [en línea]. 25 tipos de ataques informáticos y cómo prevenirlos. Ciberseguridad.blog 2018, 20 de enero. [2 de may. de 20] disponible en: https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/
- SÁNCHEZ MAIRENA, Alfonso. Memoria escrita, herramientas electrónicas y fondos archivísticos 2008 [en línea]. [Consultado el 21 de abril 2020] disponible en: https://www.aragon.es/estaticos/GobiernoAragon/Departamentos/EducacionCulturaDeporte/Documentos/docs/Areas/Actas_II_Jornadas_Aragonesas/Actas VIII jornadas de Archivos Tomo 2.pdf#page=116
- SÁNCHEZ, Arcángel Eduardo. [en línea] La gestión de documentos como estrategia de innovación empresarial. revista Venezolana de Información, Tecnología y Conocimiento, ISSN 1690-7515, Vol. 11, n. 2. [Consulta 23-9-2020]. http://produccioncientificaluz.org/index.php/enlace/article/view/18873
- Seguridad de la Información en Colombia. [sitio web] Marco legal de Seguridad de la Información en Colombia. Seguridadinformacioncolombia.blogspot.com: 2010, veintitrés de febrero. [consultado 19 de abr. de 20] disponible en: http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html
- Seguridad informática. [en línea] Jhonsar: 2010. [consultado: 2 de may. de 20] disponible en: https://www.blogger.com/profile/11714127096787219444
- SGSI. ISO 27001: Funciones y mecanismos de salvaguarda. [en línea]. Pmg-ssi.com: 2017, 27 de abril. [consultado: 4 de mayo de 2020]. Disponible en https://www.pmg-ssi.com/2015/04/iso-27001-funciones-y-mecanismos-de-salvaguarda/
- SISTEMA INTEGRADO DE CONSERVACIÓN. [en línea]. Supersolidaria.gov.co: 2016. [Consultado el 20 de abril 2020] disponible en: http://www.supersolidaria.gov.co/sites/default/files/public/data/sistema_integrado_de_conservacion_2016_sic.pdf
- Software de digitalización de documentos. [Consultado el 24 de marzo de 2021] disponible en: https://www.alarisworld.com/es-es/solutions/software/documentscanningsoftware#section%202
- SQLMap. Herramienta Automática de Inyección SQL. [sitio web]. [Consultado el 21 de abr. de 20]. Disponible en: https://www.dragonjar.org/sqlmap-herramienta-automatica-de-inyeccion-sql.xhtml
- Technical Guidelines for Digitizing. [sitio web] Cultural Heritage Materials Creation of Raster Image Files. 2016, septiembre. [consultado: el 19 de mayo de 2020] Disponible en: http://www.digitizationguidelines.gov/guidelines/FADGI%20Federal%20%20Agencies%20Digital%20Guidelines%20Initiative-2016%20Final_rev1.pdf

- Tipos de bases de datos y las mejores bases de datos del 2016. 2015, noviembre 18. [sitio web] [Consultado el 24 de marzo de 2021]. Disponible en: https://blog.pandorafms.org/es/tipos-de-bases-de-datos-y-las-mejores-bases-de-datos-del-2016/
- Tramullas. [sitio web]. Tendencias en documentación digital 2008. [consultado el 24 de marzo de 2021]. Disponible en: http://eprints.rclis.org/13051
- Vulnerabilidades importantes que afectan la seguridad de bases de datos en las empresas [sitio web]. Onasystem: 2020. [consultado 21 de abr. de 20] disponible en: https://www.onasystems.net/wp-content/uploads/2016/09/Bases-de-datos-Vulnerabilidad.