MODELO PREVENTIVO DE SEGURIDAD DE INFORMACIÓN APLICADO A LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS CON VALOR PROBATORIO

ANDREA CAROLINA BUSTOS SANTOS

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE COMUNICACIÓN Y LENGUAJE
DEPARTAMENTO DE CIENCIA DE LA INFORMACIÓN
CARRERA DE CIENCIA DE LA INFORMACIÓN – BIBLIOTECOLOGÍA
BOGOTÁ D.C.
2017

MODELO PREVENTIVO DE SEGURIDAD DE INFORMACIÓN APLICADO A LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOSCON VALOR PROBATORIO

ANDREA CAROLINA BUSTOS SANTOS

Trabajo presentado como requisito para optar al título de
Profesional en Ciencia de la Información – Bibliotecólogo

Director: M.Sc. Germán Eduardo Torres Hernández

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE COMUNICACIÓN Y LENGUAJE
DEPARTAMENTO DE CIENCIA DE LA INFORMACIÓN
CARRERA DE CIENCIA DE LA INFORMACIÓN - BIBLIOTECOLOGÍA
BOGOTÁ D.C.2017

"La universidad no se hace responsable de los conceptos emitidos por sus alumnos en sus proyectos de grado

.

Sólo velará porque no se publique nada contrario al dogma y la moral católica y porque los trabajos no contengan ataques o polémicas puramente personales. Antes bien, que se vea en ellos el anhelo de buscar la verdad y la justicia".

ARTICULO 23 DE LA RESOLUCIÓN No. 13 DE JUNIO DE 1946

Agradecimientos

“La mejor forma de predecir el futuro es crearlo” -Peter Drucker

Quiero agradecer a Dios por permitirme llegar a esta etapa de mi vida y darme la oportunidad de construir este sueño lleno de buenos recuerdos y momentos de enorme felicidad.

*De forma especial quiero agradecer a todos mis amigos, colegas y maestros por acompañarme en la construcción de este camino. En especial a German Torres por ser un pilar en este proceso, g*racias por aportar en mi crecimiento profesional, estoy segura que es el inicio de grandes proyectos juntos.

A mis padres, Gilma Santos y Dagoberto Bustos por brindarme ese apoyo incondicional en cada etapa e inculcarme el valor del conocimiento desde mis primeros años de vida. Gracias por confiar en este sueño y por apoyarme incondicionalmente en la construcción de mi camino como profesional integral. Sé que no ha sido fácil, pero agradezco a Dios y a la vida por contar con su amor y apoyo infinito. Hoy es nuestro logro gracias y mil gracias.

Quiero agradecer a toda mi familia, por su apoyo incondicional, en especial a mi hermano por ser un gran ejemplo de perseverancia a quien le guardo profunda admiración, a toda mi familia, por la motivación y el cariño, y a mi compañero incondicional de esta larga travesía, Sergio, gracias por confiar en mí, en este sueño y por ser mi gran apoyo 1.825 días llenos de una profunda eudaimonia.

Andrea

Dedicatoria

Un viejo amigo solía decir “cuanto mayor es el obstáculo, mayor es la gloria de superarlo”. A mis padres, seres únicos y excepcionales, este triunfo es de ustedes.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

AGN: Archivo General de la Nación

CAdES: Advanced Electronic Signatures

CIA: Consejo Internacional de Archivos

CNUDMI: Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional

Documento Electrónico de Archivo: "Es el registro de información generada, recibida, almacenada y comunicada por medios electrónicos, que permanece en estos medios durante su ciclo vital; es producida por una persona o entidad en razón de sus actividades y debe ser tratada conforme a los principios y procesos archivísticos"[1]

Firma digital: "Método de valor numérico que se adquiere a un mensaje de datos estrechamente vinculado a la clave del iniciador y al texto del mensaje" [2]

Firma Electrónica Avanzada: Según la directiva europea, se define como aquella que cumple con los siguientes requisitos: 1) estar vinculada al firmante de manera única 2). Permitir la identificación del firmante 3). Haber sido creada utilizando

[1] Acuerdo No. 060. *Por el cual se establecen pautas para la administración de las comunicaciones oficiales en las entidades públicas y las privadas que cumplen funciones públicas.* 30 de octubre 2001.

[2] Ley 527. (1999). *Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.* 1999, 18, Agosto

medios que el firmante puede mantener bajo su exclusivo control 4). Estar vinculado a los datos que se refiere de modo que cualquier cambio ulterior de estos sea detectable. [3]

Firma Electrónica: "método de seguridad informática y documental asociado a la incorporación de datos en forma digital que permiten las funciones de autenticidad, integridad y no repudio respecto al contenido del mensaje de datos" [4]

HASH: Algoritmo matemático único que se le atribuye a un objeto digital en función de corroborar la secuencia del valor asignado en su estructura.

IF: Informática Forense

Mensaje de Datos: "La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax"[5]

MODE: Metadatos obligatorios para el documento electrónico

PAdES: Advanced Electronic Signature)

PGD: Programa de Gestión Documental

SGDEA: Sistema de Gestión de Documentos electrónicos de Archivo

TSA: Sellado de Tiempo

UNESCO: Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

XAdES: (XML-Advanced Electronic Signature)

[3] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. (2001). Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno
[4] Peña, D. (2015). *De la firma manuscrita a las firmas electrónica y digital.*
[5] Ley 527. (1999). *Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.* 1999, 18, Agosto.

INTRODUCCIÓN

En la actualidad el concepto de documento ha sufrido una transformación terminológica y funcional que ha ido evidenciándose en el desarrollo de nuevos procesos y productos en la gestión documental. Aun así, la evolución del concepto se ha modificado por el desarrollo tecnológico en el mundo de la información. Categorizando una nueva perspectiva de documento en función del campo electrónico, siendo este, un componente más de la gestión de documentos.

De esta manera que, la transformación digital y las nuevas tendencias tecnológicas han acarreado grandes cambios hermenéuticos, a partir de la relación del sujeto con el contexto y en este caso en particular en la creación, gestión e intervención en el mundo de los documentos de archivo. Por esta razón, la relación convergente del documento en el ámbito electrónico ha constituido una dinámica de transformación que ha posibilitado el desarrollo de nuevos procesos y tácticas de negocio, que resultan estratégicas para las organizaciones que han decidido apostar por esta nueva corriente de la archivística.

Es por esto que el desarrollo del presente trabajo de grado está orientado a propuestas que buscan establecer buenas prácticas entorno al documento electrónico desde tres corrientes correlacionales al objeto de estudio, en este caso, la ciencia archivística, jurídica e informática. Por tanto, se plantea una propuesta innovadora que busca identificar el valor del documento electrónico desde su etapa de creación hasta su disposición final. De esta manera, se busca crear una propuesta heurística de las propiedades del documento en el tiempo, junto con la seguridad de la información, que se materializara en las empresas colombianas que optaron por una certificación en la ISO/ NTC27001: 2013 y han establecido protocolos de buenas prácticas, como lo es el Programa de Gestión Documental (PGD) que se encarga de normalizar los procesos documentales a nivel organizacional.

En este orden de ideas, la gestión de los documentos electrónicos es crucial para establecer una cadena de relaciones en función de un modelo emergente que busca, estar fundamentado en la naturaleza del documento que ha sido producido en un entorno netamente tecnológico. A diferencia de los documentos en físico y de los actuales sistemas híbridos que son el reflejo de gran parte de las organizaciones colombianas. Según Cruz (2003) “La gestión de los documentos electrónicos no concluye en este momento de transición, sino que continúa con el gran reto que representan los sistemas íntegramente electrónicos” (p6).

Por consiguiente, se debe dimensionar la concepción misma del documento como calidad de testimonio siendo una característica fundamental dentro de los diferentes procesos de relación entiéndase sujeto- documento. Siendo este pilar, el principal aspecto jurídico que busca establecer la validación frente al valor probatorio del mismo en función del documento electrónico. Como expresa Fuster (1999) “Los documentos de archivo son reflejo de las funciones y actividades del hombre, producto y testimonio de una gestión. De ahí la nota fundamental que puede atribuírseles y que es la objetividad” (p.5) es decir, que el documento debe poseer unas propiedades que garanticen que es único, autentico e íntegro.

Sin embargo, el desarrollo de estos procesos y el grado de importancia en las organizaciones, lamentablemente es otro. En la actualidad no se han percatado de evaluar todas las vertientes que engloban la gestión de documentos electrónicos y más en función de garantizar las propiedades del documento en el tiempo. De manera que, la inseguridad de la información dentro de este entorno, ha ocasionado el incremento de la delincuencia informática y la inestabilidad de los sistemas de información en las organizaciones. Por lo tanto, la rápida expansión de las tecnologías ha creado un ecosistema digital que permea el desarrollo de procesos fraudulentos en diferentes estancias de negocio. Siendo, el documento el primer objeto de prueba ante un hecho. Como consecuencia, se permite afirmar que el presente estudio dará una claridad teórica sobre el desarrollo de buenas

prácticas enfocado en disciplinas que convergen hacia un mismo objeto de estudio, en este caso el documento electrónico.

Por lo tanto, para poder establecer una correlación terminológica adecuada que permita establecer una propuesta heurística entorno a la gestión de los documentos electrónicos en una línea de tiempo, se debe tener una convergencia entre la seguridad de la información, el campo jurídico y la ciencia documental. Por consiguiente, se procede a estructurar el presente trabajo de grado en cinco (5) capítulos, expuestos de la siguiente manera:

En el **Capítulo I**, se identifica y caracteriza antecedentes históricos, contextuales, empíricos y teóricos entorno a la gestión de los documentos, ya que, por medio de los objetivos propuestos y el desarrollo estructural y coherente de la temática, se busca justificar de manera objetiva y racional un escenario de construcción de problemáticas emergentes, propósito por el cual se fundamenta la presente investigación.

En el **Capítulo II**, se establece la metodología que se llevara a cabo para el desarrollo del trabajo en mención, se estipula que tipología de investigación es la más adecuada permitiendo identificar una contextualización con la temática a partir de la identificación de categorías y subcategorías apriorísticas. Posterior a esta etapa, se realiza un proceso de revisión bibliográfica que permita identificar hallazgos relevantes para el propósito de la investigación. Finalmente, se establece instrumentos para la recolección de datos que permita analizar variantes de asociación de la información recopilada y de esta manera construir referentes teóricos.

En el **Capítulo III,** se realiza un análisis e interpretación de la información recopilada que se considera pertinente para los objetivos del estudio. De esta manera, se construye una discusión teórica entorno a diferentes postulados por autores de gran influencia en la ciencia documental, informática y jurídica. Permitiendo establecer un hilo conductor en función de una construcción teórica

entorno al objeto de estudio desde una visión nacional e internacional, siendo esto el marco teórico, producto de esta construcción académica.

En el **Capítulo IV**, se propone una solución metodológica que responde a la pregunta de investigación, que tiene por objetivo la construcción de un modelo conceptual que permita identificar y asegurar las propiedades del documento electrónico en el tiempo gracias a la correlación con la seguridad de la información y el soporte estructural desde el campo jurídico. Por lo tanto, se establece postulados de buenas prácticas que busca otorgar una solución que garantice estos retos emergentes en el campo archivístico y en los entornos organizacionales.

En el **Capítulo V**, se expone de manera exhaustiva los hallazgos y resultados obtenidos a los interrogantes propuestos en la investigación, con la finalidad de exponer recomendaciones que permitan desarrollar los procesos y funciones de manera armónica teniendo en cuenta la problemática y los objetivos expuestos.

CAPITULO I

1. PLANTEAMIENTO DEL PROBLEMA

En las últimas décadas, la sociedad mundial y especialmente el contexto colombiano ha sufrido una transformación histórica entorno a la era digital que ha permeado el surgimiento de nuevos procesos y modelos dentro del campo empresarial, específicamente en las áreas de gestión documental y el proceder archivístico. Siendo este último resultado de la actual revolución de información digital, ya que, desarrolla un accionar a partir de principios tecnológicos de gestión e implementación que han posibilitado nuevos modelos de estructuración de datos e información.

Con este enfoque, se retoma del proceder documental los sistemas de gestión de documentos electrónicos (SGDE) ya que estos, tienen por su funcionalidad un grupo de sistemas de información centrados en la gestión de documentos de origen electrónico en el campo archivístico. Por consiguiente, se desarrolla una evidencia en el contexto colombiano que permite ejemplificar el manejo inadecuado de la documentación en diferentes entornos organizacionales.

Lamentablemente, en la actualidad se ha visto vulnerados procesos y procedimientos, dentro de las entidades a causa del desconocimiento de buenas prácticas en la gestión archivística lo cual afecta el desarrollo eficiente de los procesos dentro de las unidades. Sin ir más lejos, se retoma la Registraduría Nacional del Estado Civil Colombiana, ya que, según cifras del periódico El Tiempo (2015) para el año 2015 alrededor de 3.146 personas ha denunciado en la Capital de la República la falsificación de documentos y posterior suplantación de identidad.

Acto que permite constatar irregularidades y falencias en la gestión de buenas prácticas en entidades que no solo afecta a la organización en particular, sino, a las personas naturales y jurídicas que tengan alguna relación vinculante, ya sea de manera interna o externa. En resumidas cuentas, se evalúa las deficiencias del ciclo de vida del documento en relación con sus principios de originalidad y orden de procedencia que afectan la seguridad y trazabilidad en un contexto documental.

Para ejemplificar, la Registraduria Nacional del Estado Civil da a conocer a la ciudadania una comunicación oficial, que permite dar cuenta de los procesos en el marco de la identificación ciudadana, teniendo en cuenta irregularidades en el manejo documental:

> En la actualidad los registros civiles de nacimiento, matrimonio y defunción, sus copias y las certificaciones son expedidos y entregado a los ciudadanos en un papel que no ofrece todas las garantías de seguridad que impidan su falsificación, y además dificulta el control eficiente del recaudo cuando se efectúa este trámite. (Registraduría Nacional del Estado Civil, 2012, p1).

De acuerdo a lo anterior, se tipifica un proceder sustentado bajo normatividades que no salvaguardan la integridad y seguridad de los documentos en el tiempo y que no garantizan una evidencia probatoria. Por esta razón, se retoma la terminología de buenas prácticas específicamente en el campo documental ya que la autenticidad e integridad de la información, son temáticas interrelacionadas con el proceder de actividades organizacionales.

No obstante, dentro del marco normativo colombiano se adapta la Norma NTC/ISO 15489 – 1 que establece características esenciales de los documentos electrónicos, para que estos sirvan de prueba dentro de las entidades, teniendo en cuenta las siguientes características: autenticidad, fiabilidad, disponibilidad e integridad. Siendo este último, el referente del documento electrónico que desarrolla principios cuyo fin es garantizar el carácter probatorio a partir de

principios de seguridad y no alteración de los contenidos en el tiempo, prevaleciendo su disposición final.

Sin embargo, la falsificación, suplantación y modificación de documentos son actividades recurrentes a nivel corporativo. A causa de esto, la mayoría de organizaciones se contradicen con los parámetros normativos de buenas prácticas que establecen los organismos internacionales y nacionales. Dicho de otro modo, no se articula de manera coherente la política documental con la normativa. Para ilustrar mejor, se retoma el caso de la constructora brasilera Odebrecht acusada por millonarios desfalcos que contribuyen la corrupción en América Latina, en especial en el contexto colombiano por la construcción de la "Ruta del Sol" ya que, se encuentran varios dirigentes del país involucrados.

En particular, se destaca las irregularidades del Banco Agrario de Navelena que es investigado por la Fiscalía General de la Nación. Según se afirma en un artículo publicado por Caracol Radio:

> La solicitud del crédito por fue hecha por $ 100.000 millones, pero sin explicación, a la Junta Directiva del Banco Agrario se le solicitó aprobar un monto de $ 120.000 millones, lo que se hizo el 12 de noviembre de 2015 con condiciones para su desembolso para proteger los recursos (Caracol Radio, 2017, p.1).

En este orden de ideas, se evidencia la modificación del contrato de la obra subscrito con el Banco Agrario, lo cual, abre un gran interrogante sobre las deficiencias en materia de seguridad, transparencia e integridad de la información materializada en documentos electrónicos que se ven alterados bajo delitos de corrupción y fraude.

Teniendo en cuenta lo anterior, no se cumple el principio de buena fe que se establece en la Ley de Transparencia y Derecho Acceso a la Información Pública y Nacional 1712 de 2014 que establece que "En virtud del cual todo sujeto obligado, al cumplir con las obligaciones derivadas del derecho de acceso a la información

pública, lo hará con motivación honesta, leal y desprovista de cualquier intención dolosa o culposa". Por lo tanto, la transparencia es entendida como un medio cual se integran derechos fundamentales de información y divulgación, acto que no se ha visto reflejado en los últimos acontecimientos empresariales en el campo colombiano, producto de procesos de alteración, falsificación y duplicidad de documentos en función pública y privada.

En este mismo sentido, se considera que la normativa colombiana tipifica de manera exhaustiva la funcionalidad de los sistemas de gestión documental de las empresas de manera probatoria, sin embargo la aplicación en el tiempo es cuestionada. Como afirma Navas y Torres (2011) "Se encuentran normas de carácter técnico cuya finalidad es la gestión de la información; al respecto, la familia de las Normas ISO 27000, centrado en los Sistemas de Gestión de Seguridad de la Información" (p.63). Sin retomar el rol fundamental de las tecnologías de información y comunicación como carácter probatorio de buenas prácticas de gestión.

Esto impulsa procesos en las organizaciones, para que obtén por certificarse en la ISO 27000 como elemento articulador de seguridad de información y tratamientos electrónicos de los contenidos estratégicos y administrativos de las entidades. Por lo tanto, la ISO 27000 no puede desligarse de los procesos y políticas documentales en función de buenas prácticas. Teniendo como resultado, el manejo de la evidencia digital que debe garantizar políticas de seguridad de información y datos entendiéndose desde la dimensión de la información estructura y no estructurada dentro de las tecnologías que faciliten los sistemas de gestión de información que permitan detectar evidencias de alteración o vulneración de los contenidos digitales. Por consiguiente, resulta pertinente analizar los procesos que se disponen en relación a un documento durante su ciclo de vida. Se tiene como base teórica el desarrollo de lineamientos que permiten que los documentos electrónicos de archivo en su naturaleza histórica

presenten un tiempo de retención mayor sin presentar riesgos de distinta índole que afecte la integridad, autenticidad y disposición final del documento.

Por ejemplo, se trae a colación el escándalo de corrupción política más polémico de las últimas décadas, el famoso Carrusel de la Contratación que se evidencio en la administración del año 2008 al 2011 por el ex alcalde de Bogotá Samuel Moreno Rojas en el año 2010. A causa de este fenómeno se afectó gravemente la capital Colombiana en materia recursos políticos, económicos y sociales entre otras vertientes. Por ende, se retoma la Sentencia SP14623-2014 emitida por la Corte Suprema de Justicia al proceso adelantado contra el ex Senador Néstor Iván Moreno Rojas por participar en los retrasos e irregularidades en la contratación de obras públicas. Para corroborar lo anterior, se expone evidencia de la prueba en la sentencia emitida por la Corte Constitucional:

> Igual sucede con el contador John Octavio Tirado Acosta, quien manifestó que la firma que aparece en el documento referido por Miguel Nule no es la suya, lo que lo lleva a inferir que muy seguramente fue creado ilícitamente en el departamento de licitaciones de los Nule, oficina en la cual se falsificaron documentos, tal como lo reconoció Mauricio Galofre. (Corte Suprema de Justicia, 2014, p.51).

De acuerdo a lo anterior, esta problemática es resultado de un mal manejo documental desde la suplantación, alteración y posterior fraude de la documentación. Por consiguiente, el objeto estructural del valor probatorio que se expone como eje articulador del hecho vinculante del acusado con el delito, se denomina documento probatorio. Hechos delictivos que incurren en falsedad ideológica que según la Corte Constitucional cuestiona la veracidad de un documento auténtico. En este caso en particular, la Sentencia emitida contra Néstor Iván Moreno Rojas permite identificar vínculos acreditados a un proceso probatorio como los documentos que fueron encontrados como elemento vinculante dentro del proceso judicial, convirtiéndose en una prueba documental.

Paralelamente, permite cuestionar la veracidad, tratamiento y principios de los documentos electrónicos teniendo como eje de análisis, la documentación a nivel general dentro de entornos organizacionales, en este caso particular el Instituto de Desarrollo Urbano (IDU) que no solo vincula al proceso al acusado, sino, a diferentes actores políticos que participaron en este desfalco a la capital. Por ende, las irregularidades nacen acciones fraudulentas, producto de un mal tratamiento de documentos reflejo desde la visión archivística como alteración de las propiedades de los contenidos. Sin embargo, se destaca un mal manejo de una política documental y un inadecuado tratamiento de los documentos en el entorno organizacional, ya que no se verifica sus principios desde su nacimiento hasta su disposición final, siendo objeto de prueba y posterior cuestionamiento en cualquier periodo de tiempo. Como afirma Redondo (2009) “la comprensión de los procedimientos es la clave para la comprensión de los sistemas de información en los que están incluidos estos documentos electrónicos” (p.392).

Ante esta situación, el contraste desarrollado con pruebas digitales es dependiente de una interpretación rigurosa de sus contenidos. Por lo tanto, la integridad de datos y la capacidad de análisis e interpretación de las evidencias serán esenciales para la clasificación de documento electrónico probatorio. Por esta razón, se deben tener en cuenta la trazabilidad digital como afirma Prayudi (2015) "Cada contacto deja un rastro" a partir de una visualización, acceso y conexión con el sistema interno y externo en consideración con el contexto de la evidencia digital.

Por lo expuesto, en este contexto, es necesario analizar el principio de integridad a partir de un modelo preventivo dentro del campo de estudio de la archivística, dimensionado desde una visión interdisciplinar con la seguridad informática que posibilite la integración y creación de procesos. Permitiendo una implementación con las empresas colombianas para que optimice procesos y salvaguarde el valor probatorio de los documentos electrónicos.

En la actualidad, no se regula de manera preventiva la producción y gestión delos documentos electrónicos teniendo en cuenta toda la trazabilidad desde su producción y adecuada gestión como mecanismos enfocados en la integridad de los sistemas de gestión de documentos electrónicos de archivo (SGDEA) Teniendo en cuenta normatividad que permita el desarrollo eficiente de buenas prácticas, procesos y procedimientos articulados bajo la teoría de seguridad de información como elemento convergente y de asociación entre áreas complementarias, como lo es la ciencia archivística y la seguridad informática.

Llegando al punto de proponer el siguiente interrogante ¿Cómo desarrollar un modelo preventivo de seguridad de información que favorezca la gestión de documentos electrónicos integrando buenas prácticas informáticas y archivísticas? En relación a lo anterior, este proyecto permitirá una aproximación teórica y metodológica que hace visible la utilización de procesos de seguridad de información y archivística para la producción de nuevos planteamientos entorno a esta temática.

1.1. JUSTIFICACIÓN

El uso masificado de las tecnologías informáticas en la actualidad ha permeado el desarrollo de nuevos modelos dentro del marco de las organizaciones, trayendo como consecuencia preocupaciones en torno a la seguridad informática y el tratamiento adecuado de la gestión de la información. Debido a que, por el desconocimiento de buenas prácticas, muchos de los procesos en materia documental se encuentran vulnerables ante el alto nivel de volatilidad y el riesgo de amenazas no deseadas.

Se propone un modelo enfocado en la gestión de documentos electrónicos resultado de una propuesta interconectada con la seguridad de información que permita describir una serie de fases de aplicación en el campo documental de naturaleza electrónica, a partir de un mecanismo que garantice la protección y vigencia de la documentación en el tiempo. Por consiguiente, la investigación se concentra en un alto componente holístico, debido a que posibilita la incorporación de elementos a través de los cuales se pretende priorizar las fases de identificación, observación, análisis e interpretación de los instrumentos de control en materia de levantamiento de información.

Sumando, un estudio analítico frente a la gestión de documentos electrónicos garantizado en el tiempo sus características fidedignas desde el estado de producción y su posterior disposición final, interconectando disciplinas desde la dimensión archivística, jurídica e informática. Por esta razón, es indispensable que

la organización colombiana se encuentre certificada en la norma técnica ISO 27000 para que se aplique de manera estructural el modelo del presente estudio, teniendo en cuenta, las características de implementación de los Sistemas de Gestión de Seguridad de Información. Lo cual permita fortalecer los procesos de convergencia entre estas ciencias interconectadas producto de buenas prácticas en el mundo informacional.

Por tal motivo, se indaga en posibles soluciones preventivas aplicadas al sector empresarial colombiano desde una visión interdisciplinar de la ciencia de la información y la seguridad informática. Sin embargo, en el proceso de aplicación de la presente propuesta se busca analizar los resultados desde un ámbito informático, que aporte soluciones prácticas y verídicas. Por lo tanto, se utiliza una validación académica con instrumentos tecnológicos que convergen con la disciplina informacional e informática, teniendo como resultado la verificación de distintos procesos en los que se ha visto involucrado el documento electrónico, como se evidencia desde la disciplina forense:

> Los expertos en informática forense compiten con la alta volatilidad de la evidencia digital, ya que las pruebas pueden ser borradas o alteradas como parte de la acción criminal. La problemática se acrecienta debido a que las técnicas forenses actuales no son escalables. El procesamiento de datos es una labor que demanda tiempos elevados, los medios de almacenamiento de información son cada vez más grandes y el secuestro de material informático va en constante aumento. (Gómez, 2014, p.3)

Teniendo como resultado, una propuesta centralizada en un modelo de seguridad de información enfocado en las características fidedignas de los documentos electrónicos en el tiempo. Que evidencia elementos probatorios desde el campo de la evidencia digital para corroborar sus propiedades fidedignas del objeto digital. De esta manera, se fortalecerán las buenas prácticas de gestión de documentos electrónicos en convergencia con la seguridad de información y el proceder desde la evidencia digital para optimizar el manejo de la integridad de

los documentos en el sector empresarial. Determinando procesos, prácticas y manejo de la información desde una visión interdisciplinar.

1.2. PREGUNTA DE INVESTIGACIÓN

¿Cómo desarrollar un modelo preventivo de seguridad de información que favorezca la gestión de documentos electrónicos acorde a la integración de buenas prácticas informáticas y archivísticas, y que mantenga el valor probatorio del mismo a través de tiempo?

1.3. OBEJTIVOS

Objetivo General

- Crear un modelo preventivo de seguridad de información aplicado a la gestión de documentos electrónicos de archivo integrando buenas prácticas con el fin, de aplicar una contribución al manejo a las propiedades fidedignas de los documentos electrónicos en el tiempo en el marco de las organizaciones colombianas.

Objetivos Específicos

- Establecer instrumentos de seguridad de información aplicado a los documentos electrónicos de archivo.
- Integrar buenas prácticas archivísticas en el manejo de seguridad de información garantizando las propiedades fidedignas del documento electrónico en el tiempo.
- Determinar los procesos de la gestión de los documentos electrónicos acorde al proceder informático, creando mecanismos de seguridad que garanticen los procesos organizacionales de manera transparente.
- Justificar el valor probatorio de los documentos electrónicos de archivo desde un modelo que integre buenas prácticas documentales.

CAPITULO II

FUNDAMENTACIÓN METODOLÓGICA

2. Investigación documental

2.1. Introducción al desarrollo del método

La presente investigación se desarrolla con un propósito académico que tiene por objetivo proponer una convergencia entre requerimientos funcionales y estratégicos en el campo de la ciencia archivística, jurídica e informática, específicamente en el marco de las organizaciones colombianas como eje articulador de buenas prácticas. Siendo el documento electrónico fundamento de análisis y discusión de la pesquisa a desarrollar. Por consiguiente, la investigación se centra en un método cualitativo de tipo documental, categorizado con enfoque descriptivo.

De tal modo, que la articulación de los elementos anteriormente descriptos se vinculen a empresas colombianas que cuentan con un Programa de Gestión Documental y una certificación en la Norma Técnica Colombiana ISO 27000 enfocado en los Sistemas de Gestión de la Seguridad de Información, siendo este componente un resultado de buenas prácticas que favorece la estructuración del modelo a desarrollar.

Por lo tanto, se establece un método cualitativo que se relaciona dentro de un conjunto de postulados con un enfoque que busca conceptualizar sobre derivados teóricos expuestos ante la relación del sujeto con el contexto, teniendo como finalidad la construcción de conocimientos de manera coherente y constructiva.

El método en mención permite en primera instancia, establecer un análisis histórico -comparativo Bernal (2006), ya que el procedimiento de investigación permite establecer las características esenciales de cada fenómeno a estudiar, teniendo como resultado un análisis de semejanzas, que consiste en establecer la relación de dichos fenómenos, infiriendo en una conclusión que converge con un origen en común (p.57). En este caso, el estudio se enfoca desde las propiedades originarias y legitimas del documento de archivo teniendo en cuenta su concepción etimológica, enmarcado por el proceso de hibridación al campo electrónico.

En segunda instancia, se destaca el método analítico – sintético que según Bernal (2006) “estudia los hechos, partiendo de las descomposición del objeto de estudio en cada una de sus partes para estudiarlas de forma individual (análisis) y luego se integran dichas partes para estudiarlas de manera holística e integral” (p.57) en este orden de ideas, se desarrolla una investigación estructural enfocada desde los principios de los documentos electrónicos en función jurídica, documental e informática. Por ello, se permite conocer y describir el estado actual de la gestión documental desde la normatividad aplicada a los sistemas de gestión de documentos electrónicos dentro de las organizaciones colombianas.

Ahora bien, dentro de la categorización de la investigación a desarrollar se realiza una combinación de dos tipos: documental y descriptiva debido a que en algunas ocasiones no solo se centra en el desarrollo de un único método sino, que busca establecer una relación para el análisis de los datos, en el área de estudio a desarrollar. Hernández, Fernández & Baptista (1998) ratifican que:

> Una investigación puede caracterizarse como exploratoria, descriptiva, correlacional o explicativa pero no solo situarse en un componente único, aunque el estudio se centre en el campo exploratorio, en la mayoría de los casos contara con elementos descriptivos o bien un estudio documental incluirá elementos descriptivos, todo en un mismo contexto interconectado.

En definitiva, se construye un contexto teórico basado en documentación académica y normatividad con fundamentación nacional e internacional enfocado en la gestión de documentos electrónicos en el campo organizacional colombiano, por ende, el método documental permite establecer un estudio detallado, sistemático y metodológico que posibilita el rastreo de diferentes fuentes documentales, con el objetivo, de corroborar el corpus del presente estudio.

2.2. Etapa de identificación de elementos necesarios para la investigación

De acuerdo con el objetivo de la investigación, que está centrado en la construcción de un modelo conceptual que permita identificar la relación de tres áreas de estudio se tiene como objetivo, establecer buenas practicas, enfocados en los documentos electrónicos en las organizaciones colombianas. Por lo tanto, es de gran importancia identificar los ejes temáticos que hacen parte del desarrollo metodológico de la presente investigación, ya que, de acuerdo al proceso de investigación documental se desarrollara un hilo conductor y secuencial que permitirá la construcción teórica de la investigación en mención.

Se retoma el enfoque desde la Ciencia de la Información como disciplina que se correlaciona con todos los campos de análisis debido a que, la línea de investigación está enmarcada desde parámetros de organización y gestión de la información, ya que, el desarrollo de estrategias enfocadas en áreas de desarrollo tecnológico posibilita procesos de información y comunicación. Lo cual, permite fundamentar el área de la documentación y la archivística a partir de la apropiación y sistematización de los procesos. Por consiguiente, esta línea de investigación permite evidenciar un escenario de análisis, enfocado en la gestión de la información desde cualquier entorno organizacional teniendo en cuenta su aplicabilidad en diferentes áreas.

2.3. Etapa de revisión bibliográfica

Inicialmente, se identifica un análisis inductivo y deductivo implícito en la metodología a desarrollar. En primera instancia, se establece palabras claves que permitan recolectar información de textos individuales asumiendo un análisis que nace de lo particular a lo global a partir de una sistematización. Teniendo en cuenta lo anterior, se establecen tres etapas de análisis:

En la primera etapa se realiza un levantamiento de información que responde a un estudio de exploración de contenidos académicos coherentes con la temática a desarrollar. Por lo tanto, siguiendo el proceso de la investigación documental se realiza una retrospectiva que hace referencia a estudios previos enfocados en la gestión de los documentos electrónicos desde la ciencia archivística y la transversalidad con el proceder jurídico e informático.

La segunda etapa consiste en establecer instrumentos que permitan la recolección de datos con el objetivo, de identificar variables de asociación enfocadas al estudio descriptivo para realizar una correcta planificación de las categorías apriorísticas a investigar. Para contextualizar, se realizó un rastreo en las siguientes bases de datos académicas: Web of Science, Ebsco Host, Redalyc, Scielo, Dialnet y E-brary. Finalmente, se empleó una organización estructural por medio del gestor bibliográfico EndNote.

En la tercera y última etapa se analizan las tres grandes categorías apriorísticas del presente estudio: Ciencia archivística, la seguridad informática y la ciencia jurídica todas en convergencia con el documento electrónico. Como consecuencia, se realiza un análisis de la información con el objetivo de reunir los componentes esenciales que constituyen el corpus de observación e investigación. Por lo tanto, se emplea el proceso de triangulación hermenéutica que posibilita un análisis estructural enfocado en tres subcategorías que son correlacionales con todas las áreas a investigar. Para tal efecto, se construye un instrumento en el que se ubican las categorías y subcategorías en

Columnas que permite inferir características y autores destacados en cada componente, y a su vez procesos emergentes que son resultado de la triangulación a partir de la correlación dialéctica de la información recopilada.

Dentro del proceso de la investigación documental se debe tener como eje estructural del método, la revisión bibliográfica en función de constatar el estado actual de la producción académica. Con el objetivo, de realizar un análisis exhaustivo de los contenidos pertinentes para el presente estudio. De manera que, la técnica de muestreo utilizada corresponde a criterios por parte del investigador, ya que, el método no es probabilístico (Bernal, 2006). Por lo cual, el modo que se emplea permite escoger criterios y juicios establecidos por el investigador lo cual incide en el muestro y los elementos de selección. En este contexto, la revisión de literatura resulta crucial para establecer una objetividad y dar un soporte teórico al documento en desarrollo. Como expresa Hernández, et al., (1998)

> Con frecuencia las ideas son vagas y deben traducirse en problemas más concretos de investigación, para lo cual se requiere una revisión bibliográfica sobre la idea. Esta revisión es importante aun cuando nuestro enfoque sea puramente cualitativo. Ello, sin embargo, no impide que adoptemos una perspectiva única y propia (p.39).

En este orden de ideas, se establece fases jerárquicas partiendo desde un componente global como los es en este caso, la gestión documental que subcategoriza procesos y programas enfocados en las buenas practicas desde una visión generalizada. Por tanto, da cuenta del proceso originario del documento desde la concepción etimológica y sus características esenciales teniendo en cuenta, autores de influencia anglosajona y latinoamericana.

Para continuar con este hilo conductor, se desarrollan elementos que se relacionan con la ciencia documental. Para ejemplificar, se realiza una revisión detallada de la diplomática documental y el valor probatorio de los documentos desde un análisis archivístico y jurídico. Sin dejar de lado, componentes que,

correlacionados con estas dos áreas de estudio, permiten establecer una revisión exhaustiva.

Finalmente, se realiza una búsqueda enfocada en la seguridad informática y elementos esenciales dentro de los procesos documentales en el campo electrónico para poder llegar a unir componentes en la creación del modelo a desarrollar.

2.4. Recolección de datos

Una vez realizado el proceso de análisis bibliográfico, se llega a la fase deductiva que busca analizar, interpretar y evaluar los resultados obtenidos de los datos e información recopilada, ya que a partir de aprehender e interpretar de manera coherente y relacional el contenido recopilado posibilita la construcción de una base teórica estructurada.

Para tal fin, se emplearon instrumentos de búsqueda estratégicos que permitieron manejar los listados bibliográficos en función de establecer un orden secuencial de los contenidos encontrados en la investigación. Con el objetivo, de establecer una línea de trabajo que permitiera denotar las categorías apriorísticas del presente estudio.

En primera instancia, dentro de la categoría de la ciencia archivística se estableció búsquedas en las siguientes bases de datos: Ebsco Host, Redalyc, Scielo, Dialnet y E-brary. Cabe destacar que la mayoría de las publicaciones se encuentra categorizadas dentro del contexto Latinoamericano. Por ende, se estableció una normalización de términos, debido a las diferencias conceptuales en traducciones del idioma inglés.

Para ejemplificar, se retoma la traducción y contextualización del concepto “Documento” ya que, presenta una variación en su significado. Como afirma Cruz (2009) “transposición del término cuando procede del inglés, lengua para la que el equivalente *document* tiene un significado genérico y para designar el documento

tal cual lo entiende la archivística, emplea la *voz record* y aún en ocasiones la *voz archive*" (p.30). Por lo cual, permite destacar la diferenciación terminológica en los diferentes contextos de aplicación. Sin embargo, en ocasiones se entiende el documento desde una generalidad aplicado a un formato lo cual, incide en el proceso de hibridación al concepto de documento electrónico.

Como consecuencia, se realizó una búsqueda exhaustiva sobre las diferencias terminológicas ya que, la aplicación del término puede variar en las fuentes documentales de consulta y su interpretación puede no articularse adecuadamente. Como expresa Cruz (2009) "La voz document se reserva para designar la acepción genérica de toda información registrada sobre un soporte" (p.30). Esto permite inferir la diferenciación con el concepto *Records* tiene una asociación al valor probatorio perse del documento en función de evidencia y prueba documental. La gestión de los documentos electrónicos es crucial para entender procesos y funciones documentales en entornos organizacionales, así pues, que debe ser riguroso el estudio que se realice entorno a ellos.

En vista de esto, se efectuó una revisión detallada de la producción académica entorno a los documentos electrónicos y sus categorías teniendo en cuenta, postulados archivísticos en el ámbito nacional e internacional. En el que se establece un autor base para el desarrollo de la presente investigación, si bien, se retoman postulados de varias autorías. Este, en particular presenta una gran influencia y liderazgo.

Se identificó al autor Cruz Mundet José Ramón con mayor grado de relevancia y producción en la ciencia archivística como ente rector a nivel internacional. Debido a que, sus contenidos académicos presentan un gran impacto e influencia en la producción de literatura latinoamericana y anglosajona entorno al campo documental. De esta manera que, se establece un marco de tiempo de dos décadas para identificar la línea de interpretación de diferentes autores y contextos entorno a la funcionalidad de las propiedades de un documento original que permita evidenciar su valor probatorio.

En relación a lo anterior, se destaca el proceder jurídico que permite evidenciar el valor probatorio de los documentos desde la normativa nacional e internacional y su validez en el ámbito documental e informático, ya que, partir de la recolección de datos se identificaron elementos estratégicos para el desarrollo del modelo. Teniendo como autor rector de la corriente jurídica a Peña Valenzuela Daniel que permite realizar un análisis de correlación con el documento electrónico.

En este punto, se confluye el método documental con el enfoque descriptivo ya que, se relacionará a partir de un marco de tiempo y una normalización de términos que da soporte para la definición de la técnica y el análisis comparativo con el instrumento a mencionar. Por lo tanto, dentro del proceso de investigación se realizó una búsqueda enfocado en la categoría apriorística de Seguridad de la Información.

Por ende, se empleó el gestor bibliográfico EndNote desarrollado por la compañía de información Thomson Reuters en la base de datos multidisciplinar Web of Science como primer instrumento de investigación.

A continuación se evidencia en la Tabla No.1 las fuentes encontradas en la base de datos Web of Science en la que se empleó criterios de búsqueda centralizados en la seguridad de la información, protección y seguridad en entornos empresariales y casos de estudio del área en mención, para extraer componentes que sirvan de estructura para la construcción teórica. Sin dejar de lado, los filtros aplicados en categorías, áreas temáticas, tipologías de documentos e idiomas para refinar la búsqueda y encontrar contenido de relevancia.

TABLA DE SINTESIS DE REVISIÓN BIBLIOGRAFICA					
Nº de Fuente	**Categoría**	**Tipo de Fuente**	**Titulo**	**Autor (es)**	**Año de publicación**
1	Information Science - Library Science	Revista: Profesional de la Información	Information security management: A bibliographic review.	Cardenas Solano, L.J	2016
2	Computer Science Information Systems	Revista: Ijispm-International Journal of Information Systems and Project Management	A process framework for information security management.	Haufe, K.	2016
3	Computers & Security	Artículo de Revista	A network based document management model to prevent data extrusion.	Morovati, K.	2016
4	Computer Journal	Revista: Computer Journal	An End-to-End Security Approach for Digital Document Management.	Munoz Hernandez, M.D	2016
5	Computers & Security	Artículo de Revista	Implementing information security best practices on software lifecycle processes 15504 Security Extension.	Mesquida, A. L	2015
6	Computer Science	Revista: International Journal of Critical Infrastructure	Blind information security strategy.	Sveen, F.O	2009

		Protection			
Nª de Fuente	**Categoría**	**Tipo de Fuente**	**Título**	**Autor (es)**	**Año de publicación**
7	Computers & Security	Artículo de Revista	Information Lifecycle Security Risk Assessment: A tool for closing security gaps.	Bernard, R.	2007
8	Computer Science	Revista: Bell Labs Technical Journal	Using the bell labs security framework to enhance the ISO 17799/27001 information security management system.	McGee, A.R	2007
9	Information Science - Library Science	Revista: Information and Management	Digital signature: use and modification to achieve success in next generational e- business processes.	Gupta, A.	2004

Tabla 1. Matriz de referencias bibliográficas en EndNote

Fuente: Elaboración propia. (2017).

En este proceso de inferencia, se delimita la información en un marco de tiempo de quince (15) años para identificar el grado de actualización entorno a la categoría de Seguridad de Información empleando términos de búsqueda relacionados al tratamiento, creación y seguridad de la información en entornos organizacionales. Lo cual, permite constatar una gran influencia al campo de la computación informática en convergencia con los procesos de negocio. Sin dejar de lado, el alto nivel de producción bibliográfica en el idioma inglés, ya que, la normalización de terminologías resulta crucial en la base de datos Web Of Science.

2.5. Análisis comparativo de fuentes

Investigación Documental		Propiedades de un Documento Electrónico de Archivo			
Categorías	**Fuentes**	**Autenticidad**	**Integridad**	**Disponibilidad**	**Confiabilidad**
Ciencia Archivística	Norma Técnica Colombiana ISO 15489-1: 2001	Un documento de archivo auténtico es aquél del que se puede probar: a) que es lo que afirma ser; b) que ha sido creado o enviado por la persona que se afirma que lo ha creado o enviado; c) que ha sido creado o enviado en el momento que se afirma.	Completo e inalterado.	Es aquél que puede ser localizado, recuperado, presentado e interpretado. Su presentación debería mostrar la actividad u operación que lo produjo.	Sus contenidos pueden ser creídos como una representación exacta y completa de las transacciones, actividades o hechos de los cuales dan fe y seguridad, así durante su desarrollo, como en transacciones o acciones futuras. Sus contenidos son fidedignos.
Ciencia Jurídica	Firma electrónica Daniel Peña Valenzuela	Documento original: fuente primaria de información con todos los rasgos y características que permitan garantizar su autenticidad e integridad Autenticidad respecto al Código General del Proceso Articulo 244 el documento, se original o copia,	Atributo de la información que hace referencia a que el documento está completo, no ha sido objeto de modificación, alteración,	Prueba documental: puede ser reforzada con la adecuada gestión documental mediante marcos de referencia, estándares técnicos, y normas de autorregulación que sirven de fundamento para las buenas	Según la Corte Suprema de Justicia: la confiabilidad está vinculada a los atributos técnicos del mensaje de datos que garanticen su integridad, inalterabilidad, recuperabilidad y rastreabilidad.

		es auténtico cuando existe certeza sobre la persona que lo ha elaborado, manuscrito o firmado, así como respecto de quién es el iniciador en caso de envió del mismo o cuando exista certeza respecto a la persona a quien se le atribuyo el documento.	tacha o falsificación.	prácticas de gestión documental.	
Categorías	**Fuentes**	**Autenticidad**	**Integridad**	**Disponibilidad**	**Confiabilidad**
Ciencia Informática	Norma Técnica Colombiana ISO 27000	Puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad	Propiedad de salvaguardar la exactitud y estado completo de los activos	Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.	Preservación de la confidencialidad , la integridad y la disponibilidad de la información.
Peritaje Informático	Evidencia Digital Jeimy J, Cano	Entendida como aquella característica que muestra la no alterabilidad de los medios originales, busca confirmar que los registros aportados corresponden a la	Al contar con mecanismos y procedimient os de control de integridad se disminuye la incertidumbre sobre la	Completitud/sufi ciencia se centra en toda la evidencia necesaria para adelantar un caso.	La confiabilidad nos dice si efectivamente los elementos probatorios aportados provienen de fuentes que son creíbles y verificables.

		realidad identificada en la fase de identificación y recolección de evidencia.	manipulación no autorizada de la evidencia aportada.		

Tabla 2. Esquema de componentes holísticos.

Fuente: Elaboración propia. (2017).

2.6. Etapa de identificación de elementos necesarios para la investigación

De acuerdo a la tabla 2. Se evidencia las categorías generales de la investigación en convergencia con las propiedades del documento electrónico. Para llegar a obtener este resultado, se empelo el proceso de triangulación hermenéutica que consiste en la reunión terminológica a partir de una relación pragmática de toda la información recopilada que resulta coherente con la investigación. De modo que, se asume un trabajo de interpretación riguroso entorno a las categorías y subcategorías apriorísticas para poder realizar un proceso deducción racional significativo entorno a la información recopilada. Para obtener los resultados evidenciados en el esquema de componentes holísticos, se realiza una serie de pasos para llegar al proceso de triangulación hermenéutica. En primera instancia, como se observaba en la recolección de datos se realiza una selección de información. Posterior a esto se elabora una categorización de tópicos que convergen con el propósito del estudio. Finalmente, para continuar con el proceso de cada componente se identifica características de las áreas a investigar para realizar la respectiva triangulación con cada estamento y sus componentes relacionales. Con el objetivo, de analizar la información recopilada se aplica el

proceso de triangulación que permite crear comparaciones entre categorías y determinar campos de investigación que estén abiertos a investigaciones futuras.

En consecuencia, se emplearon palabras claves enfocadas en la gestión de los documentos electrónicos, valor probatorio, diplomática documental, ciclo de vida del documento, documento de archivo, propiedades de los documentos, conservación, buenas prácticas, políticas de gestión, seguridad de la información, firma electrónica, autenticidad, mensaje de datos, integridad, disponibilidad, evidencia digital, entre otras. Como se evidencia, estos son algunos de los términos empleados en el proceso de recopilación de información con la finalidad, de identificar mecanismos de asociación de las categorías apriorísticas del presente estudio. Por lo tanto, se emplean tres subcategorías apriorísticas que permiten identificar el valor probatorio de los documentos electrónicos: autenticidad, integridad y disponibilidad.

MARCO TEÓRICO - CONCEPTUAL

3. Introducción a los campos de investigación

3.1. Contextualización

La manifestación y desarrollo del entorno digital ha permeado un crecimiento exponencial en la gestión de documentos, especialmente en el ámbito electrónico en las organizaciones. Producto de la creación de nuevos mecanismos que optimizan el buen proceder documental. Por lo tanto, para el desarrollo de la presente investigación se hace una aproximación teórica acorde a visiones interdisciplinares que convergen en este campo de estudio. De acuerdo a esto, para efectos del desarrollo de este proyecto se tendrá en cuenta el aporte de autores que desarrollen una perspectiva enfocada en la gestión documental electrónica en relación con la evidencia digital forense, permitiendo maximizar el campo de aplicación de la presente investigación.

Así, por ejemplo, la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) y el Consejo Internacional de Archivos (CIA) han propiciado el desarrollo a nivel organizacional. Es por esta razón, que se desarrolla un trabajo a la luz del tratamiento de documentos electrónicos en confluencia con la seguridad documental, con el objeto de crear mecanismos de control para optimizar procesos y conseguir resultados probatorios.

3.2. Gestión Documental

En la actualidad, las empresas y organizaciones reconocen a la información como activo fundamental, para el desarrollo de actividades y procesos internos y externos que se desarrollan mediante el manejo y tratamiento documental. Según el Archivo General de la Nación (AGN, 2000) define la Gestión Documental como “Conjunto de actividades administrativas y técnicas tendientes a la planificación, manejo y organización de la documentación producida y recibida por las entidades, desde su origen hasta su destino final, con el objeto de facilitar su

utilización y conservación" (p.1). En este orden de ideas, la gestión documental juega un rol fundamental en la creación, mantenimiento, uso y posterior disposición del contenido documental

3.2.1. Programa de Gestión Documental (PGD)

Todas estas observaciones se relacionan con la creación de un Programa de Gestión Documental (PGD). Siendo este último, un mecanismo que le proporciona a la organización un desarrollo secuencial de la documentación desde su origen hasta su disposición final. En relación con lo anterior, el Programa de Gestión Documental según el Archivo General de la Nación, puede ser visto, como:

> Instrumento archivístico que formula y documenta a corto, mediano y largo plazo, el desarrollo sistemático de los procesos archivísticos, encaminados a la planificación, procesamiento, manejo y organización de la documentación producida y recibida por la entidad, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación. (Archivo General de la Nación, 2014, p. 10).

Desde este punto de vista, permite realizar un análisis detallado frente al deber ser de las organizaciones en materia documental, que posibilita una apropiación de políticas documentales que favorece procesos y resultados en este campo. Considerando el proceder instrumental del Programa de Gestión Documental, ya que, se debe resaltar su carácter reglamentario por la Ley 594 de 2000 y el Decreto 1080 de 2015 del Ministerio de Cultura en el que se establece que el programa es esencial para la gestión de información dentro de las entidades a nivel nacional.

3.2.2. Gestión de información en el campo documental

Para las organizaciones el Programa de Gestión Documental en convergencia con la gestión de información, da a conocer una visión estructural enfocada en un funcionamiento conjunto de políticas, procesos y procedimientos que busquen la

toma de decisiones eficientes dentro de márgenes administrativos, técnicos y legales.

Por lo tanto, la convergencia de estos dos parámetros según Horton pueden ser vistos como:

> Conjunto de instancias responsables de la definición de acciones y políticas relacionadas con aspectos como la forma en que la información: se adquiere, registra y procesa; y en que además se usa y se comunica; también se ocupa en el cómo los integrantes o personas que manejan la información, aplican sus habilidades y cooperan entre ellas. (Horton, 1979).

En este orden de ideas, la gestión de información en relación con el (PGD) permite la creación de un instrumento estratégico que garantiza procesos de planificación desde una sostenibilidad acorde a fases de implementación que permite generar un instrumento transversal a las dependencias de las entidades.

3.2.3. Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA)

De este modo, se realiza una conexión conjunta con el Sistema de Gestión de Documentos electrónicos de Archivo (SGDEA). En primera instancia, se retoma del proceder documental electrónico ya que estos, tienen por funcionalidad un grupo de sistemas de información centrados en la gestión de documentos de origen electrónico en el campo archivístico. Como afirma Mastropierro (2008) “Sistema computarizado corporativo que maneja documentos para mejorar todo el proceso informacional. Está integrado por la aplicación específica de gestión de diferentes aplicaciones que soportan en forma complementaria el proceso de gestión documental electrónica” (p.153-154).

En segunda instancia, la gestión de documentos es el resultado de una integración global de la ciencia archivística, sin dejar de lado los documentos en físico en este componente documental.

> Sin embargo, y al igual que ha sucedido con los documentos en papel, su reconocimiento como función archivística no ha partido del reparto competencial de las organizaciones, sino de la ocupación por la vía de los hechos, primero, y con un reflejo normativo a la vista de las soluciones aportadas, después. (Cruz, 2003, p. 6).

3.2.4. Sistemas Híbridos

Resulta pertinente, analizar y evaluar la situación persistente en las organizaciones, ya que, aun es habitual encontrar sistemas mixtos, es decir, etapas transicionales de los documentos físicos y electrónicos en el campo empresarial. Siendo un reto emergente, por su proliferación de formatos y contenidos. Según el postulado de Cruz (2003) “Estos sistemas mixtos plantean la necesidad de mantener vinculados documentos y sistemas dispares en la secuencia lógica (legal o de negocio), de acuerdo con la cual han sido creados, y que es imprescindible para evidenciar y probar las actividades que recoge” (p.6).

En resumen, los sistemas mixtos no solo representan un riesgo en su unificación total, sino su gran protagonismo en el ámbito de la autenticidad y conservación, ya que, la evaluación no solo se realiza desde la dimensión física, sino, desde la inminente necesidad de un sistema de seguridad en el mundo de los documentos electrónicos como fenómeno emergente.

3.3. El concepto de documento

No obstante, el activo esencial de las organizaciones son los documentos. Pero resulta de gran importancia delimitar el concepto de documento, ya que, puede variar acorde al campo interdisciplinar en el que se esté evaluando, en este caso, se retoma el concepto desde la visión archivística, específicamente documento de archivo. Etimológicamente procede del latín *documentum,* que en una visión muy amplia sirve como fuente de conocimiento que busca probar y demostrar algo. Sin

embargo, en la actualidad la terminología se relaciona intrínsecamente con el campo jurídico.

3.3.1. Documento desde la visión jurídica y archivística

Paralelamente, el concepto de documento se puede dividir en dos grandes clases como expresa Fuster (1999) “desde su naturaleza exclusivamente jurídica, que engendran derechos y obligaciones, y de naturaleza administrativa, que no tienen naturaleza jurídica pero que sin embargo son documentos testimoniales, auténticos, objetivos y, por tanto, verídicos o fehacientes” (p.104).

> Según el Código de Procedimiento Civil artículo 251 Son documentos los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares.

En concordancia, se retoma el Código Penal artículo 294 que define documento como: “cualquier medio mecánico o técnicamente impreso, soporte material que exprese o incorpore datos o hechos, que tengan capacidad probatoria”. Asimismo, el diccionario de terminología archivística de Mastropierro (2008) define documento como “testimonio material de un hecho o acto realizado en el ejercicio de sus funciones por personas físicas o jurídicas, públicas o privadas, de acuerdo con unas características de tipo material y formal” Se hace una definición más amplia atendiendo a caracteres esenciales con las organizaciones.

3.3.2. Caracteres del documento

3.3.2.1. Caracteres externos

Cruz (2012) refiere que a mediados del siglo XX Theodore Roosevelt Schellenberg normalizo dos características fundamentales de los documentos. En primer orden, se encuentran los caracteres externos relacionados con su estructura específicamente, es decir, el modo empleado para transmitir información entiéndase documentos en forma oral o escrita, textual, iconográfica, sonoros, audiovisuales y electrónicos.

3.3.2.2. Caracteres internos

En segunda instancia, se encuentran caracteres internos relacionados con el contenido que busca destacar la autenticidad e imparcialidad acorde a parámetros administrativos y jurídicos de las entidades productoras destacando características sobre los orígenes funcionales especificados en el contenido del documento.

3.4. Valores y propiedades de los documentos en función probatoria

De esta manera que, se hace mención a los valores de los documentos que resultan intrínsecamente relacionados desde su creación hasta su disposición final. Por lo tanto, se amplía el proceder de la doctrina archivística en relación con el campo jurídico permitiendo afirmar la validez del documento, como valor probatorio. Como expresa Fuster (1999) “Los documentos son testimonio e información y pueden ser utilizados como prueba y como fuente de datos” (p.105) Es decir, que los documentos permiten dar cuenta de los procesos y funciones de los individuos entorno a su valor probatorio.

A causa de esto, se destaca el concepto de autenticidad vinculado con la prueba, producto del documento original. Esto permite afirmar que posee características esenciales del término documento el cual debe tener una prueba científica para su valoración, destacando claro está, su valor diplomático. Por lo tanto, para dimensionar el desarrollo documental desde una perspectiva de prueba se debe esclarecer como la comunicación se vuelve un elemento crucial en el desarrollo del ser humano. Siendo este, el que analiza y desarrolla mecanismos de

interpretación y comunicación de hechos, actividades y pensamientos por medio del habla y posterior el desarrollo de signos en la escritura.

3.4.1. De la grafología a la prueba documental

Las civilizaciones, han tenido un desarrollo evolutivo que analiza la dinámica particular de los individuos con los signos, ya que se crea un perfil único que se vuelve intransferible del sujeto, expresado por medio de la escritura. Postulados como los del filósofo italiano Camilo Baldo afirma que la escritura es la manifestación del hombre.

> La palabra hablada, por tanto, es el reflejo de un pensamiento, pero la palabra escrita es algo más, es una copia pura del pensamiento en la que se puede ver las discrepancias entre lo que realmente siente la persona y lo que quiere expresar. (Robles, 2015, p.253).

En definitiva, se converge estas asociaciones con la grafología que según la Real Academia de la Lengua Española (RAE) se define como: "Arte que pretende averiguar, por las particularidades de la letra, cualidades psicológicas de quien la escribe. Siendo categorizada como una ciencia, que busca dar cuenta de una finalidad de identificación" Esto posibilita, el análisis de la escritura acorde a la vinculación que se realiza con un hecho producto de una relación sujeto – prueba corroborado en los escritos, siendo una ciencia que permite traer actores vinculantes en referencia a este proceder. Convirtiéndose en un fundamento científico que se sustenta, bajo el termino de pericia caligráfica. Nace bajo la proliferación constante de alteración de documentos producto del desarrollo de técnicas para prevenir, detener y demostrar pruebas de alteración de documentos en materia de seguridad.

3.5. El concepto de documento electrónico

El escenario que se ha desarrollado hasta el momento, ha permitido construir un referente teórico y contextual del concepto documento, sin embargo, la realidad circundante ha traído consigo una transformación tecnológica en el campo de la información y comunicación. Lo cual, permite acuñar el término documento electrónico según el postulado de Cruz Mundet (como se citó en Cruz, 2011) lo define como "el documento generado, gestionado, conservado y transmitido por medios electrónicos, informáticos o telemáticos, siempre que incorporen dos firmados electrónicamente" (p.148).

En el contexto legal colombiano el Acuerdo No. 060 de (2001) específicamente en el artículo segundo puntualiza documento electrónico como:

> Registro de información generada, recibida, almacenada y comunicada por medios electrónicos, que permanece en estos medios durante su ciclo vital; es producida por una persona o entidad en razón de sus actividades y debe ser tratada conforme a los principios y procesos archivísticos. (p.2)

En relación a lo anterior, el documento electrónico cumple una pieza clave dentro de las organizaciones categorizándose como un elemento de valor estratégico dentro de las distintas instancias en las que se encuentre involucrado. Por tal motivo, se retoma el documento electrónico como medio de prueba, es decir, como se expresa en el artículo No. 10 de la Ley 527 de 1999:

> Admisibilidad y fuerza probatoria de los mensajes de datos. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria.

Siendo categorizado, dentro de un marco normativo a partir de una valoración jurídica que permea al mensaje de datos entendido en este caso como documento electrónico una validez probatoria para el desarrollo de distintos procesos.

3.5.1. Características del documento electrónico desde la Norma Internacional ISO 15489-1

No obstante, dentro del marco normativo colombiano se adapta la Norma Internacional ISO 15489 -1 Información y documentación – Gestión de documentos específicamente en el apartado 1 generalidades se establece características fundamentales de los documentos electrónicos, para que estos sirvan de prueba dentro de las entidades, teniendo en cuenta las siguientes características: autenticidad, fiabilidad, confiabilidad e integridad. Siendo este último, el referente del documento electrónico que desarrolla principios cuyo fin es garantizar el carácter probatorio a partir de principios de autenticidad, integridad y confiabilidad de los contenidos en el tiempo, prevaleciendo su disposición final acorde a un protocolo de seguridad.

3.5.2. Propiedades de los documentos electrónicos

En este orden de ideas, el documento electrónico presenta unas características y propiedades que sean mencionados anteriormente como principio probatorio. Por lo tanto, se debe destacar el contexto de aplicación del documento para analizar su estructura en partes integrales, ya que, como expresa Cruz Mundet (2012) “Para considerarlo completo y autentico el documento debe conservar su estructura originaria” (p. 61) Aun así, la terminología de integridad de los documentos se encuentra asociada la originalidad de los documentos. Como afirma Cano (2010) “No obstante, sin importar la falta de normativa al respecto, se puede decir que un documento por el simple hecho de ser autentico goza de integridad, pero no necesariamente un documento considerado íntegro tendrá las características de auténtico” (p.73). A continuación, se procede a establecer un

cuadro de conceptualización sobre las propiedades estructurales por diferentes autores dentro del campo archivístico.

PROPIEDADES	CONCEPTUALIZACIÓN	AUTOR
Autenticidad	"Que los documentos sean inmunes a todo tipo de manipulación y alteración a lo largo del tiempo. Así mismo que evidencien la procedencia." (2009)	Cruz Mundet José Ramón
	"Como evidencia de que el origen de las informaciones contenidas en un documento y fijada sobre un soporte determinado, en este caso electrónico, son ciertas. " (2007)	Díaz Rodríguez Alfonso
	"comprobarse que el documento es lo que afirma ser, ha sido creado o enviado por la persona de la cual se afirma que lo ha creado o enviado; y que ha sido creado o enviado en el momento en que se afirma" (2017)	Nani Forte
Integridad	"Que mantengan íntegros y completos su estructura y contenido." (2009)	Cruz Mundet José Ramón
	" Que garantice que las informaciones contenidas en el documento electrónico no han sufrido alteraciones durante la transmisión entre distintos sistemas tanto dentro de los sistemas de la misma organización donde se generó el documento electrónico" (2007)	Díaz Rodríguez Alfonso
	"Se refiere a que el contenido de un documento es completo y esta inalterado. Los documentos deben estar protegidos contra modificaciones no autorizadas." (2017)	Nani Forte
	" Que los documentos puedan demostrar los efectos que	Cruz Mundet

Fiabilidad	contienen, es decir, que tengan un contenido fidedigno" (2009)	José Ramón
	"Asegura que el contenido de dicho documento es una representación completa y precisa de las operaciones, las actividades o los hechos de los que da testimonio" (2017)	Nani Forte
Disponibilidad	"Que sean recuperables para su uso en todo momento y circunstancia" (2009)	Cruz Mundet José Ramón
	"Característica que permite localizar, recuperar, presentar e interpretar el documento. Su presentación debe reflejar el contexto en el que ha sido creado "(2017).	Nani Forte

Tabla 3. Definiciones de propiedades estructurales de los documentos electrónicos. Fuente: Elaboración propia (2017).

3.5.3. Gestión de documentos electrónicos

Para el desarrollo funcional de los documentos electrónicos se debe tener en cuenta, la naturaleza que estos ejercen en el ámbito empresarial en relación a sus procesos. Por ende, el uso operacional y detallado de los mecanismos de trazabilidad, permite crear una correlación terminológica con el concepto de gestión de documentos electrónicos, término acuñado por la archivística para determinar los procesos de creación del documento a partir del ciclo de vida y su relación con diferentes variables que se articulan dentro de la dinámica misma del documento. Como afirma Cruz (2009) "la gestión de los documentos electrónicos es un aspecto más de la gestión de los documentos, entendida como una función archivística global que la integra" (p.36)

Incluso, se debe tener en cuenta la naturaleza propia del documento electrónico en relación a su uso y diseño, ya que, a partir de un buen protocolo desde la visión archivística, permite garantizar las propiedades del documento desde una fase

holística, es decir, una integración de todos sus componentes que aseguren su utilización . Por lo cual, se debe tener en cuenta la funcionalidad y uso de los mismos para el desarrollo de las actividades dentro de las organizaciones.

Por lo tanto, se entiende que la gestión de documentos electrónicos dimensiona una claridad mayor entorno al contexto de aplicación, ya que, como expresa Cruz (2003) “pone el énfasis en la naturaleza de los documentos, creados, utilizados y conservados en entornos tecnológicos” (p.6). En este sentido, se debe crear una integración de todos los componentes archivísticos que permitan confluir en este proceso al campo electrónico. De esta manera que, se debe tener en cuenta las propiedades de los documentos electrónicos como elemento estructural ya que, deben permitir una organización estratégica entorno al proceder y utilización de los documentos.

3.6. De la diplomática a la prueba documental

La concepción de la diplomática se asocia desde una visión congruente que permite relacionar su proceder a procesos vigentes en la actualidad dentro del marco documental permitiendo corroborar su grado de importancia en relación a la veracidad de los contenidos. De ahí que, los documentos presenten una diplomática centrada en un carácter formal en su estructura lógica, ya que, proporciona un conocimiento a priori del tratamiento documental enfocado en documentos electrónicos. Se analizan elementos formales enfocados en la autenticidad desde una visión verídica. Trayendo a colación el concepto de diplomática como una ciencia en auge en esta investigación.

> La Diplomática es una ciencia antigua que se ha utilizado para analizar los documentos archivísticos con el fin de determinar sus caracteres internos y externos, establecer su tipología y determinar la autenticidad de los documentos, con el fin de averiguar si los derechos y los hechos que contenían eran verdaderos o falsos. (Bermúdez, s.f, p.1)

Sin embargo, esto permite la creación de premisas enfocadas en la identificación de la validez probatoria del documento en este orden de principios, ya que, debe estar completo e inalterado. Siendo este último, el segundo principio en hacer mención dentro del marco de documento electrónico, denominado integridad. En contraste se hace mención, al tercer componente que permite realizar un acercamiento hermenéutico del documento al sujeto a partir de la relación documento electrónico- contexto, denominado confiabilidad.

En consecuencia, se contempla el documento electrónico como objeto de prueba, por ende, se debe garantizar la seguridad de información en cada fase del programa de gestión de documentos. Teniendo en cuenta, los principios de: integridad, confiabilidad y autenticidad

3.6.1. Valor probatorio

El valor probatorio de los documentos electrónicos se tiene que dimensionar desde un ámbito relacional, ya que, la aproximación teórica de documento en el ámbito jurídico hace referencia a la representación de un hecho, independientemente del formato en el que se encuentre. Por lo tanto, la vinculación del documento con el sujeto en mención entiéndase desde la intervención humana, resulta crucial para determinar cualquier tipo de prueba.

De este modo, se debe diferenciar la concepción de documento desde el ámbito físico y electrónico, ya que, en el campo jurídico y documental las características son correlacionales. Rodríguez (Citado por Pinochet, 2002) establece que un “documento informático no es un documento como los demás, sino que es un documento de especial naturaleza, que requiere, para su actuación práctica, una regulación específica”. Por ende, la caracterización del documento electrónico se ha fundamentado por su valor probatorio, debido a que esta característica jurídica de los documentos es esencial.

Sin embargo, el tratamiento jurídico de la documentación no solo debe dimensionarse desde un componente físico, ya que la gestión de documentos

electrónicos busca establecer una conexión dentro de la producción y el ciclo de vida del documento, estableciendo técnicas que ofrezcan una solución enfocado al análisis documental en función del valor probatorio. Puesto que, el documento electrónico esta admitido como prueba y tiene la misma validez que un soporte escrito en un medio físico. Esto quiere decir, que tiene que gozar de los principios de autenticidad e integridad, ya que, se tiene que identificar los parámetros del documento y en qué condiciones se encuentra. Como afirma Parra (2006) “el documento es un medio de prueba, pero muchas veces puede ser objeto de prueba” (p.6).

En relación a lo anterior, en el artículo 11 de la ley 527 de 1999 establece el criterio para valorar probatoriamente un mensaje de datos, entiéndase en este contexto como documento electrónico.

> Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta Ley, se tendrán en cuenta las Reglas de la Sana Crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente, habrán de tenerse en cuenta: la confiabilidad en la forma que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en que se identifique a su iniciador y cualquier otro factor pertinente.

De modo que, para que un documento se asuma dentro del valor probatorio y tenga plena validez jurídica debe estar completo e inalterado. Por lo cual, la integridad del documento debe evidenciarse desde el momento de su creación para corroborar que no ha sido alterado bajo ningún medio, permitiendo reafirmar principios de autenticidad, confiabilidad y no repudio.

3.7. Seguridad de información

3.7.1. Aproximación teórica desde la ISO/IEC 27001: 2013

Por consiguiente, en materia de investigación la seguridad y transformación de la información digital genera un reto emergente. En este caso, desde la dimensión convergente de la gestión documental y el proceder informático. Por ende, la evolución de las tecnologías de información y comunicación (TIC) han acelerado cambios y tendencias tecnológicas que desarrollan una dinámica entorno a la evolución constante dentro de este gran ecosistema digital.

Por consiguiente, se retoma la Norma Técnica Colombiana de Tecnologías de información y técnicas de seguridad en sistemas de seguridad de información (SGSI) ISO/IEC 27001: 2013 que permite analizar cómo gestionar la seguridad de la información a nivel empresarial. Garantizando procesos a la luz de la norma como eje articulador de buenas prácticas. Definiendo el Sistema de Gestión de Seguridad de Información (SGSI) como "parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información"(p.3). Todo esto claro está, goza de principios de preservación de la integridad, confidencialidad y autenticidad.

3.7.2. El concepto de seguridad de información desde la NTC-ISO 27002

Teniendo en cuenta lo anterior, existen normatividades que permiten regular procedimientos y buenas prácticas, enfocados en técnicas de seguridad que buscan poner en marcha un sistema de gestión de seguridad de información con el objetivo, de disminuir y regular adecuadamente el debido proceder de las organizaciones. Por ejemplo, la Norma Técnica Colombiana NTC-ISO 27002 establece una visión amplia de la necesidad de la seguridad de información en entornos empresariales. Si bien es cierto, la seguridad de información permite crear una variedad de mecanismos de protección a la información contemplando protocolos que aseguren y dinamicen el riesgo en la organización.

Como se expone en la NTC-ISO 27002 "La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la

organización y, en consecuencia, necesita una protección adecuada" (p.1) es decir, se busca disminuir amenazas y reducir grados de vulnerabilidad presentes en el sistema de información. Lo cual posibilita la reducción del impacto ante un incidente de seguridad de información en la unidad.

Por consiguiente, la gestión de incidentes de seguridad de la información tiene como objeto la toma de decisiones correctivas, resultado de un reporte de eventos que debilitan y alteran el debido proceder de la información, es así, como se desarrolla una estructura que busca monitorear constantemente los incidentes de seguridad. Además, se busca establecer controles de autenticación. Como se expone en el apartado 11.5.2 identificación y autenticación de usuarios de la NTC-ISO 27002 "Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de identificación para comprobar la identidad declarada de un usuario" (p.87) por este motivo, se debe no solo dar un control adecuado al sistema, sino, a los usuarios como agentes vinculantes en el entorno informacional.

Simultáneamente, se debe validar la integridad del mensaje de datos que ha sido creado. Por consiguiente, se debe crear un control que posibilite la creación de acciones preventivas y correctivas entorno a la autenticidad y confiabilidad de los mensajes, reduciendo así los incidentes de seguridad de información. Lo cual permite retomar el concepto de confiabilidad como es definido por la NTC-5411-1 como: "propiedad de tener comportamiento y resultados previstos consistentes" siendo este último una característica fundamental de la seguridad de información que se define como "todos los aspectos relacionados con la definición, el logro y el mantenimiento de confidencialidad, integridad, disponibilidad, no repudio, trazabilidad, autenticidad y confiabilidad de la información o de los servicios de procesamiento de información".

3.7.3. El reto empresarial desde la seguridad de la información

El desarrollo en nuestro país de normas jurídicas que respondan a los problemas que surgen del fenómeno de las tecnologías de información y comunicación se destaca. La Ley 527 de 1999 constituye uno de los pocos desarrollos importantes en este sentido. Esta situación genera un grado importante de inseguridad e incertidumbre no sólo para las organizaciones, sino para también los ciudadanos, en su condición de usuarios, consumidores y titulares de datos personales. Velasco (Como se citó en Navas y Torres, 2011, p 63).

Esto permite generar un análisis que hace referencia al artículo publicado por Navas, et al., (2010) como un nuevo enfoque de la seguridad de información en el sector empresarial

> Las organizaciones la seguridad de la información es un tema que por representar intereses de contenido legal y económico, adicionales a los técnicos, no solo debe estar en manos de los ingenieros y encargados de sistemas informáticos, sino que necesita involucrar a la gerencia, que a su vez debe convocar a grupos de interés a participar activamente en la salvaguarda y uso adecuado del derecho fundamental y mayor activo: la información. (Navas, et al. 2010, p. 63).

De este modo, se busca garantizar los principios en buen proceder documental en materia de documentos electrónicos. Por lo tanto, se establece la conexión de estos componentes con la firma electrónica que presenta una validez jurídica a nivel nacional acorde a la Ley 527 de 1999, ya que, se entiende por firma electrónica

> Datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que pueden ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

3.8. Firma electrónica

Acorde al artículo 7 de la Ley 527 de 1999 la firma electrónica se le atribuye una validez jurídica en relación con otros mecanismos de seguridad y certificación, ya que, a nivel organizacional brinda beneficios a un menor costo. Se debe resaltar que cada método empleado de seguridad busca generar una confiabilidad tecnológica en materia de autenticidad e integridad de lo que se produce en el campo documental y el usuario que genera toda la cadena de relaciones en este ámbito.

3.8.1. Definición de firma electrónica

De acuerdo a la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) en el artículo 2 (2001) define “Por “firma electrónica” se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos “(p.1) por ende, se entiende desde una asociación de disciplinas en función de los principios del documento. Para ejemplificar, se retoma el postulado de Peña (2015) que expone “la firma electrónica es un método de seguridad informática y documental asociado a la incorporación de datos en forma digital que permiten las funciones de autenticidad, integridad y no repudio respecto al contenido del mensaje de datos” (p.124)

Por lo tanto, la correcta valoración de riesgos de seguridad tecnológica se puede disminuir gracias a la incorporación del método de la firma electrónica, ya que, permite que los diferentes sistemas de información digital asuman una valoración jurídica entorno al proceder a partir de mecanismos de autenticación.

En consecuencia se confirma el principio de equivalencia de la firma manuscrita a la firma electrónica, otorgándole plena validez jurídica en función de principios de autenticidad, integridad, no repudio y confidencialidad.

De acuerdo al Inciso 3, Articulo 1 Decreto 2364 de 2012 del Ministerio de Industria y comercio define la firma electrónica como:

> Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente (p.2).

De esta manera, que se debe establecer una igualdad en el tratamiento de las tecnologías aplicadas a la firma electrónica, debido a que, la funcionalidad de la firma electrónica garantiza plana validez sobre un documento electrónico en función de los principios de integridad, autenticidad y confiabilidad.

3.8.2. Estándares de firma electrónica avanzada

La funcionalidad de las firmas electrónicas ha asumido un valor crucial en el desarrollo organizacional, especialmente en la gestión de los documentos electrónicos. Asumiendo un valor de evidencia que se corrobora por el no repudio de la comunicación empleada. Entiéndase este último concepto, como una propiedad que adquiere un objeto digital al garantizarse un servicio de seguridad que evidencia la protección y no alteración del mismo.

> Garantizar el no repudio de un documento firmado es tarea difícil, aun cuando existe todo el marco tecnológico y legal necesario para ello. Dado que el no repudio es quizá una de las propiedades de los servicios de seguridad que mayor complejidad y requisitos conlleva, cualquier vulnerabilidad en los estándares subyacentes o error en la implementación concreta puede hacer repudiable cualquier firma, incluyendo aquellas realizadas con el DNI electrónico. (Hernández, González y Ramos, 2014, p.1)

Aun así, la complejidad de la seguridad en el desarrollo de estas modalidades resulta crucial para entender variantes de asociación en el campo de las firmas electrónicas. En primera instancia, se debe esclarecer la existencia de estándares que regulan las modalidades de firma y la aplicación que estas ejercen dentro del marco de seguridad. A continuación se expone algunos de los estándares que se emplean a nivel global por la aplicación de sus formatos y estructura en la firma electrónica avanzada:

- Estándar CAdES (CMS Advanced Electronic Signatures): Se caracteriza por ser el primer formato de firma estandarizado. Sus propiedades son vinculantes con grandes volúmenes de información y optimiza el firmado de un documento original atribuyendo una codificación binaria para garantizar su seguridad.
- Estándar XAdES (XML-Advanced Electronic Signature): Este estándar se caracteriza por contener mecanismos de autenticación e integridad en relación a la protección de datos e información de los objetos digitales, ya que, abala los requerimientos legales de protección de seguridad en torno al cumplimiento del no repudio. Para entender la funcionalidad del estándar, se avala por medio del formato XML en el que se emplean nodos que permiten verificar la información en cada componente.
- Estándar PAdES (Advanced Electronic Signature) : este estándar permite incorporar los datos de la firma al documento que se encuentra en formato PDF, categorizándose desde el esquema interno como el desarrollo visual de la firma, por tanto, no requiere de la incorporación de un software especializado.

Finalmente, para entender los procesos de firmado, en especial, la modalidad de firmas longevas se debe establecer los instrumentos empleados en el periodo de preservación, de acuerdo al tipo de algoritmo y a su características temporales para su posterior renovación. Unos de los elementos que juegan un papel importante dentro de los procesos de confiabilidad temporal, son las

Autoridades de Sellado de Tiempo (TSA) que permite verificar y validar la exactitud temporal de la información. Como expresa (Hernández et al., 2014)

> Un sello de tiempo certifica que la información sellada existía antes de un instante de tiempo determinado. Esta referencia temporal, incluida en el sello de tiempo, se corresponde con el momento en que la TSA firma digitalmente la estructura de datos anterior. Sellar temporalmente una firma electrónica permite que ésta pueda ser correctamente verificada en un futuro, incluso cuando el certificado empleado ha expirado o ha sido revocado con posterioridad al momento de creación de la firma, ya que el sello de tiempo establece de forma fehaciente que la firma se generó antes de dicho momento temporal (p.3).

Finalmente, las firmas longevas actúan en colaboración con los certificados digitales y el TSA para corroborar el contenido y la estructura originaria del objeto digital. La funcionalidad recae en crear capas de seguridad y un sistema de refirmado para certificar que el documento no ha sido modificado ni alterado dentro de su oficialidad.

3.9. Delitos informáticos

En el ámbito nacional la seguridad jurídica respecto al proceder probatorio de los contenidos digitales, se ha visto en creciente desarrollo en materias de procedimientos legales, informáticos y documentales. Teniendo como eje central de discusión, la tipología del delito informático colombiano bajo un ámbito jurídico que tipifica de manera explícita condiciones especiales y diferenciadas sobre esta tipología de crímenes. Como afirma Cano (2010) “No se puede pretender aplicar a rajatabla normas escritas para regular otros aspectos y otros momentos” (p.219).

La producción masiva de contenidos y el desarrollo de su alta volatilidad en medios digitales, ha incrementado la vulnerabilidad en los sistemas de información en el campo electrónico. Según el postulado de Cano (s.f) “el aprovechamiento de fallas bien sea humanas, procedimentales o tecnológicas sobre infraestructuras de

computación en el mundo, ofrecen un escenario perfecto para que se cultiven tendencias relacionadas con intrusos informáticos" (p.1). Siendo este último el referente clave, para la creación de escenarios de análisis y discusión problemas que abarca no solo una ciencia técnico – legal, sino en su totalidad un entorno interdisciplinario.

3.10. Peritaje informático

3.10.1. Definición de perito informático

Se desarrollan estrategias y acciones que cobijan los medios informáticos, con el objetivo de verificar y constatar prácticas indebidas. En vista del incremento de delitos informáticos cabe mencionar, la técnica de peritaje informático como una disciplina interconectada con el campo de la información en materia de tratamiento digital probatorio, convirtiéndose en una herramienta de valor esencial dentro del buen proceder. La creación de este perfil, no resulta nuevo, ya que, históricamente esta experticia se deriva de la visión clásica de los grafólogos.

A causa de esto el término perito proviene del latín *peritus* caracterizado por su experiencia y practicidad. En contraste, el perito informático se define según Cano (2010) "experto en el área de las tecnologías de la información que de acuerdo con el tema requerido puede ser seleccionado según su competencia y experiencia para una labor de análisis" (p.103)De esta forma el trabajo del peritaje informático, se asocia como afirma Cano (2010) "dictamen técnico y científico sobre el objeto de análisis en el cual cuenta con la experiencia y conocimiento requerido, con el fin de que a través de fuentes de información y análisis exhaustivo llegue a conclusiones que pueda sustentar" (p.104).

Sin embargo, para dar una toma de decisiones frente a la prueba que analiza el perito informático, recae la responsabilidad, sobre un juez como ente objetivo e imparcial en la manifestación de los hechos. Como expone Quijano (2006) "El juez

tiene una libertad reglada para valorar la prueba. El juez no puede contradecir las reglas de la experiencia, las reglas de la lógica, las reglas de la ciencia, ni las reglas de la técnica" (p.12). Por lo tanto, es un acto racional que busca una valoración objetiva y confiable a partir de una decisión justa sobre la prueba y la vinculación del hecho.

Por consiguiente, es de importancia retomar el impacto de los delitos informáticos que ataca el buen proceder de las organizaciones a nivel internacional y nacional han sido estudiados en diferentes campos de aplicación permitiendo ejercer un estudio detallado sobre la informática forense (IF) como nueva ciencia en desarrollo teniendo su origen etimológico en el latín Ocampo, (2010) "forensis, que significa público y su origen del latín forum que representa el foro, plaza pública donde se trataban las asambleas públicas y los juicios. Por lo tanto, lo forense se vincula con lo relativo al derecho y la aplicación de la ley" (p.90).

3.10.2. La informática forense un problema emergente

En efecto, la evidencia de los delitos informáticos ha estimulado el desarrollo de la informática forense como ciencia en crecimiento exponencial del actual siglo XXI (López et al., s.f) Las investigaciones realizadas en diferentes campos de estudio han demostrado enfoques aplicables a los sistemas de información a nivel internacional y colombiano, permitiendo dimensionar una problemática en auge dentro del proceder de buenas prácticas de seguridad de información en la empresas privadas. (Cárdenas y Fonseca, 2012).

3.10.3. Informática forense un reto emergente en la seguridad de información

Ahora bien, dentro del marco normativo colombiano se debe tener en cuenta, el exuberante crecimiento de los sistemas de información y la ocurrencia en los

delitos informáticos por parte de la población colombiana, según cifras del Departamento Administrativo Nacional de Estadística DANE (Villamizar, et al., 2014) Dentro del contexto jurídico colombiano la (IF) se emplea como un sistema de pruebas de los sistemas judiciales. Por consiguiente, se tiene como actor legal la ley 527 de 1999 de comercio electrónico Villamizar, et al… (2014) "reglamenta y define el uso y acceso del mensaje de datos, comercio electrónico, firmas digitales y empresas certificadoras" (p.13).

Sin embargo, dentro del margen normativo colombiano no se tipifica de manera exhaustiva la funcionalidad de la informática forense dentro de los sistemas de gestión documental de las empresas de manera probatoria. Como afirma Navas y Torres (2011) "Se encuentran normas de carácter técnico cuya finalidad es la gestión de la información; al respecto, la familia de las Normas ISO 27000, centrado en los Sistemas de Gestión de Seguridad de la Información" (p.63). Sin retomar el rol fundamental de las tecnologías de información y comunicación como carácter probatorio de buenas prácticas de gestión. Como expone (Villamizar, et al., 2014). Se debe resolver problemas técnicos que permitan controlar situaciones prácticas, ya que, no existe una técnica sistemática que permita mantener una fiabilidad y originalidad de las evidencias del proceder forense.

3.11. El concepto de evidencia digital

3.11.1. La evidencia digital en función de los principios archivísticos

En este orden de ideas, el concepto de evidencia digital se convierte en un eje de articulación esencial dentro del desarrollo de la presente investigación. Se vuelve una necesidad de análisis dentro del marco probatorio. Por lo tanto, se articula una investigación rigurosa entorno a la sociedad digital y la información desde la dimensión de la seguridad informática, jurisprudencia, gestión documental y evidencia digital forense.

Se retoman autores que desarrollan una visión integral y holística respecto al desarrollo de la temática. De esta forma, permite esclarecer un adecuado proceder de buenas prácticas encaminadas en el mundo de los sistemas de gestión documental electrónicos, ya que, una valoración de la evidencia digital está enfocada en lineamiento documental desde los principios archivísticos, teniendo como eje fundamental la integridad en los documentos cuando presenta las siguientes características contextualizados según Riofrío (2004) " contiene toda la información que constataba al momento de su emisión, y que desde entonces no ha sido alterado" (p.105).

Lo anterior, destaca los procesos a partir de características legales de la evidencia que presentan una asociación estructural con los principios de los documentos electrónicos. Teniendo en cuenta, su carácter probatorio desde modelos de seguridad de información, evidencias y procesos que garanticen un buen proceder.

Dentro del marco normativo colombiano, se retoma el artículo 275 del Código de Procedimiento Penal inciso 7, se identifica los elementos materiales probatorios dentro del contexto de evidencia "El mensaje de datos, como el intercambio electrónico de datos, internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la Ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen"

Esto permite, identificar propiedades emergentes dentro de la producción del documento, en su función de auténtico, como se expresa en Ley 1564 del 2012 en el Articulo 244 "Es auténtico un documento cuando existe certeza sobre la persona que lo ha elaborado, manuscrito, firmado, o cuando exista certeza respecto de la persona a quien se atribuya el documento".

Como afirma Cano (2009) "La autenticidad de la evidencia nos sugiere ilustrar a las partes de que esa evidencia ha sido generada y registrada en los lugares o los sitios relacionado con el caso" (p.108) esto, permite deducir que en los medios

electrónicos se encuentran en una mayor exposición de riesgo, gracias a su alta volatilidad y manipulación.

Esto permite corroborar el valor probatorio de los documentos, debido a la autenticidad como elemento estructural de análisis en función de la rastreabilidad del mismo. Para corroborar este postulado se retoma el artículo 247 de la Ley 1564 de 2012 por la cual se dicta el Código General del Proceso que da a conocer la valoración del mensaje de datos como “los documentos que hayan sido aportados en el mismo formato en que fueron generados, enviados, o recibidos, o en algún otro formato que lo reproduzca con exactitud”.

Por lo tanto, para garantizar este principio dentro del margen de seguridad y gestión de documentos, se procede a realizar la conexión desde la evidencia con otro elemento articulador, denominado confiabilidad, ya que, nos permite evaluar si efectivamente los elementos en materia probatoria provienen de fuentes confiables que presentan verificación dentro del proceso probatorio. Resultado, de un proceso de sincronización de estrategias de control que permean buenas practicas hacia una confiabilidad del documento electrónico como evidencia digital.

Teniendo como resultado, una convergencia en el principio de integridad. Como expone en el postulado de “El documento electrónico como medio prueba”:

> El escrito en forma electrónica está admitido como prueba con igual fuerza que el escrito en soporte papel, bajo reserva de que pueda ser debidamente identificada la persona de que emana, y que sea generado y conservado en condiciones que permitan garantizar su integridad (Quijano, 2006, p.4)

En conclusión, se buscan fortalecer los procesos de buenas prácticas dentro de las organizaciones desde la convergencia de varias disciplinas teniendo como eje articulador la ciencia de la información especialmente la gestión de documentos electrónicos como modelo centralizado con el campo de seguridad de información

y evidencias digitales desde la dimensión de la evidencia digital resultado de un estudio interdisciplinar.

> Lo anterior supone la convergencia de las practicas forenses digitales y las de seguridad de la información, una combinación y desarrollo de capacidades que buscando la minimizar la interrupción de las funciones del negocio y aumentando su resistencia a los ataques, mantenga la relevancia, pertinencia y admisibilidad de la evidencia digital. Esta nueva realidad, establece no solo una estrategia forense y de seguridad conjunta, sino acciones proactivas y de prevención que crean una plataforma de defensa que disuada a los potenciales atacantes, su tolerancia a las fallas y anticipe escenarios de investigación criminal conocidos. (Cano, 2016, p.1).

Por ende, se procede a categorizar una investigación mixta entorno a la relación a las ciencias interconectadas dentro del concepto de documento electrónico, puesto que, no solo se dimensiona desde una mirada archivística, jurídica e informática, si no, se busca fortalecer procesos y presentar un análisis frente a decisiones prácticas, que converjan en una realidad interdisciplinar.

CAPITULO IV

4. Contexto de Aplicación del Modelo

El reto emergente de las organizaciones en la actualidad recae sobre el tratamiento y la gestión adecuada de su documentación, especialmente, en materia de políticas y buenas prácticas. Debido a que el activo más importante a nivel global en las entidades, es la información, elemento estructural de la actual economía digital. Por lo cual, se debe establecer y asegurar procesos y procedimientos que salvaguarden un adecuado proceder en función de principios documentales en el campo electrónico.

Por esta razón, en el desarrollo del presente capítulo se busca profundizar y establecer buenas prácticas para el tratamiento de los documentos electrónicos en entornos organizacionales. Con el objetivo, de asegurar las propiedades del documento desde el desarrollo de su fase inicial (creación) entendiéndose desde el momento en el que el documento se vuelve oficial dentro de la cadena de producción del ciclo de vida, hasta la etapa de disposición final. Permitiendo

esclarecer, un modelo de prevención que dé cuenta de mecanismos de seguridad capturados en cada etapa de manera correlacional.

De acuerdo a lo anterior, se busca profundizar en las propiedades del documento electrónico desde su fase inicial, teniendo en cuenta aportes desde la ciencia archivística como disciplina estructural del presente estudio. Sin embargo, para el desarrollo del modelo resulta de gran importancia la vinculación relacional con la seguridad de la información para el desarrollo de un buen proceder, que asegure las propiedades en el tiempo.

En definitiva, se busca establecer un modelo que permita identificar al documento electrónico como prueba de los diferentes procesos y actividades de las organizaciones, reuniendo características y propiedades orgánicas a partir de elementos que componen requisitos esenciales del documento. Teniendo como resultado, la integración holística de las siguientes propiedades: Autenticidad, fiabilidad, integridad y disponibilidad. Características estratégicas que permiten atribuir al documento electrónico, como documento fidedigno.

Por lo cual, el cumplimiento de estos requisitos resulta crucial, en el desarrollo del presente modelo, debido a que, la continuidad de la gestión de los documentos electrónicos en los sistemas, se dimensiona más allá de una dicotomía con la seguridad de la información. Pues bien, la categorización de los documentos debe verse desde un transversalidad que agrupa elementos de gobernanza y transparencia en entornos electrónicos y organizacionales.

A continuación, se va a desarrollar el modelo conceptual a partir de una estructuración de fases con el objetivo, de evidenciar la interconexión de cada etapa con las propiedades del documento electrónico. Permitiendo constatar, la captura de seguridad de diferentes elementos y requerimientos que resultan esenciales, para cada fase del ciclo del documento en función de establecer una interoperabilidad. El desarrollo de las siguientes propuestas, buscan a portar al objeto digital (documento electrónico) un modelo de gestión que posibilite la

creación de relaciones en sistemas interconectados, permitiendo un control documental riguroso enfocado en el desarrollo de un buen proceder. Lo cual, aumentara el ahorro de tiempo y disminución de costos dentro de procesos y funciones por las organizaciones, que obtén por desarrollar esta propuesta para la gestión de los documentos electrónicos dentro de sus sistemas de información.

4.1. Propuesta de Metadatos mínimos para la gestión de documentos electrónicos en entornos organizacionales

Los metadatos son una serie de elementos que permiten que el documento electrónico goce de un contexto funcional y administrativo. De manera que, proporciona un contexto al contenido a partir de su estructuración por una serie de requerimientos que le atribuye, un valor probatorio y de confiabilidad a los objetos digitales en el desarrollo de actividades y procesos dentro de una temporalidad. Por consiguiente, resulta de gran importancia proponer un esquema de metadatos como instrumento que permita la incorporación holística de varios componentes en función de las propiedades del documento.

El presente esquema de metadatos, se basa en el esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 de la Documentación complementaria a la Norma Técnica de Política de gestión de documentos electrónicos, españoles. Que tiene como antecedente, los propuesto y empleado por el Archivo Nacional de Australia Australian Government Recordkeeping Metadata Standard Version 2.2.

Ahora bien, dentro del contexto colombiano se retoma el Acuerdo No. 05 del año 2013 emitido por el Archivo General de la Nación en el que se establece de

manera reiterativa la obligatoriedad de los Metadatos mínimos para la descripción de los documentos electrónicos de archivo.

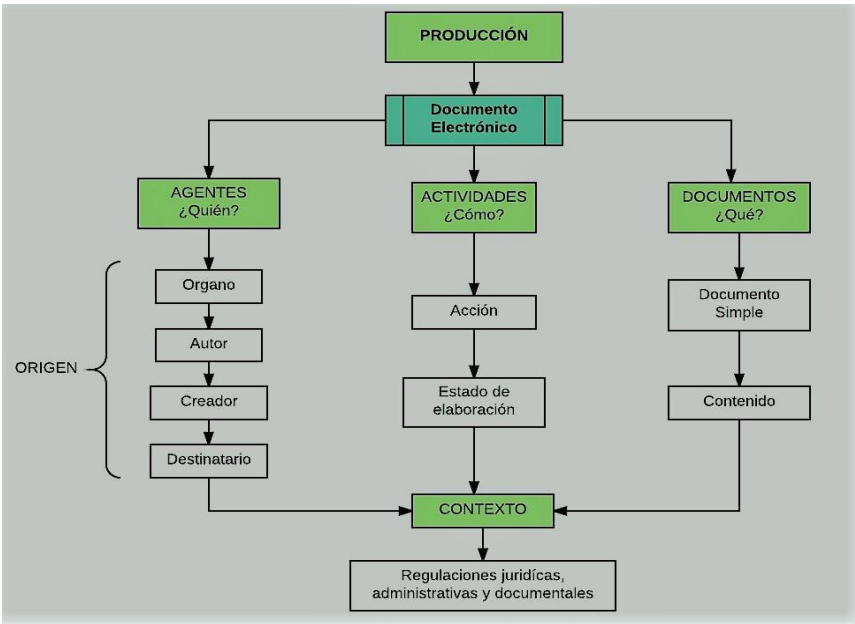

Figura 1. Entidades de los Metadatos para la Gestión de Documentos Electrónicos desde la producción. Fuente: elaboración propia. (2017), de acuerdo a la ISO 23081-1: 2016 y el Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Teniendo en cuenta esto, se evidencia cuatro tipos de entidades que resultan indispensables para la adecuada gestión de los documentos en entornos electrónicos. En primera instancia, se encuentran tres entidades relacionales en función de la producción del documento electrónico: Agente, actividad y documento entidades macro que giran entorno aun análisis secuencial dentro de los patrones que intervienen para la creación del objeto digital. Por lo cual, se establece subcategorías que son vinculantes en cada etapa que permite generar una asociación con los metadatos que se asignaran de manera estructural acorde

a la relación global. En este caso, el contexto como cuarta entidad siendo unidad de análisis que posibilita una interconexión con diferentes procesos, especialmente regulaciones en el entorno normativo.

4.1.1. Alcance del Esquema

El desarrollo del esquema de metadatos propuesto, busca establecer una convergencia entre el sistema de gestión de documentos y los procesos que se desarrollan dentro de funcionalidades de gestión en entornos organizacionales. Por lo cual, se realiza una correlación de las entidades a partir de un contexto, estructura y contenido del objeto en mención. Teniendo como resultado, la creación de documentos electrónicos fidedignos, es decir, aquellos que gozan de propiedades tales como: Autenticidad, integridad, fiabilidad y disponibilidad. Acto que se evidencia a lo largo del tiempo, optimizando las relaciones entre sistemas y componentes para intercambiar y transferir información, proceso que se materializa en el ciclo de vida del documento electrónico, a partir de la asignación de metadatos mínimos que son necesarios para asegurar el documento en el tiempo.

4.1.2. Estructura del Esquema

Como se ha expuesto en la estructura base del esquema de metadatos, presenta diferentes tipos de entidades relacionales que vinculan diferentes acciones con la gestión de los documentos en su desarrollo modular. Por tanto, resulta indispensable la creación de relaciones con otro tipo de entidades del documento para ejercer una función acorde a las regulaciones.

Seguido de esto, se debe esclarecer que las organizaciones que obtén por el desarrollo de este esquema, deben contar con una certificación en la ISO/NTC-

27001:2013 y contar con un Programa de Gestión de Documentos, ya que, el presente esquema presenta una flexibilidad que se ajusta a la implementación en diferentes sistemas, sin dejar de lado, la obligatoriedad de los requisitos mínimos establecidos en su estructura. Por tanto, presenta una compatibilidad con normas técnicas, gracias al desarrollo interoperable a lo largo del ciclo de vida del documento.

El esquema de metadatos mínimos requeridos para el documento electrónico consta de 9 elementos que se subdividen acorde al grado de implementación e importancia en la organización

- ✓ *Metadatos obligatorios para el documento electrónico (MODE) (Elaboración Propia) dentro de la categoría de principio macro:*
  i. MODE - Identificador
  ii. MODE - Órgano
  iii. MODE - Fecha de captura
  iv. MODE - Estado de elaboración
  v. MODE - Características Técnicas
  vi. MODE - Tipo documental
  vii. MODE - Firma
  viii. MODE - Trazabilidad
  ix. MODE - Seguridad

De acuerdo a lo anterior, se establece un orden jerárquico acorde a la producción del documento. Teniendo en cuenta, atributos de creación dentro del ciclo de vida del documento a partir de un orden secuencial, que evidencie la relación de las **19 sub categorías** que a su vez sub clasifican en **9 elementos** que hacen parte de los metadatos obligatorios requeridos para identificar la aplicabilidad en las diferentes etapas, en las que se busca asegurar el documento electrónico en el tiempo.

CATEGORIA DE METADATO	OBLIGATORIDAD			APLICABILIDAD			
	Obligatorio	Opcional	Condicional	Agente	Actividad	Documento	Contexto
1. Identificador	✓			✓	✓	✓	✓
1.1. Secuencia Identificador	✓			✓	✓	✓	✓
1.2. Esquema de Identificador			✓	✓	✓	✓	✓
2. Órgano	✓					✓	
3. Fecha de Captura	✓			✓	✓	✓	✓
3.1. Fecha Inicio	✓			✓	✓	✓	✓
3.2. Fecha Fin			✓	✓	✓	✓	✓
4. Estado de elaboración	✓					✓	
5. Características Técnicas	✓					✓	
5.1. Formato	✓					✓	
5.1.1. Nombre del Formato	✓					✓	
5.2. Versión del Formato	✓					✓	
6. Tipo Documental	✓					✓	
7. Firma	✓					✓	
7.1. Tipo de Firma	✓					✓	
7.1.1. Formato de Firma	✓					✓	
7.1.2. Perfil de Firma		✓				✓	
7.2. Algoritmo			✓			✓	
7.3. Valor			✓			✓	
8. Trazabilidad	✓			✓	✓	✓	✓
8.1. Acción	✓			✓	✓	✓	✓
8.1.1. Descripción de la Acción	✓			✓	✓	✓	✓
8.1.2. Fecha de la acción	✓			✓	✓	✓	✓
8.1.3. Objeto de la acción	✓			✓	✓	✓	✓
8.2. Motivo Reglado	✓			✓	✓	✓	✓

8.3. Usuario de la Acción		✓		✓	✓	✓	✓
8.4. Descripción			✓	✓	✓	✓	✓
8.5. Modificación de los metadatos			✓	✓	✓	✓	✓
8.6. Historia del Cambio		✓					✓
8.6.1. Nombre del elemento		✓					✓
8.6.2. Valor anterior		✓					✓
9. Seguridad	✓			✓	✓	✓	✓
9.1. Nivel de seguridad			✓	✓	✓	✓	✓
9.1.1. Nivel de acceso			✓	✓	✓	✓	✓
CATEGORIA DE METADATO	**Obligatorio**	**Opcional**	**Condicional**	**Agente**	**Actividad**	**Documento**	**Contexto**
9.2. Permisos			✓	✓	✓	✓	✓
9.3. Nivel de confidencialidad de la información			✓	✓	✓	✓	✓
9.4. Sensibilidad de datos de carácter personal			✓	✓	✓	✓	✓

Tabla 4. Listado de metadatos mínimos obligatorios del documento electrónico. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

4.1.3. Consideraciones de uso

Para el desarrollo funcional del presente modelo de esquema de metadatos, requeridos para garantizar las propiedades del documento electrónico se debe considerar lo siguiente:

- Las organizaciones que obtén por implementar el siguiente esquema de metadatos deben aplicar las categorías y subcategorías obligatorias, condicionales y opcionales para desarrollar una optimización de los resultados anteriormente expuesta.
- Las organizaciones no están en la obligación de implementar este esquema de metadatos dentro de sus procesos y funciones, sin embargo, deben categorizar sus protocolos de manera sincrónica con el adecuado proceder

documental en función de buenas prácticas archivísticas, informáticas y jurídicas.

4.2. Modelo metodológico de los procesos de gestión documental en correlación con la seguridad de información

Los procesos de gestión documental están relacionados al conjunto de actividades y funciones que buscan generar una vinculación de los documentos de archivo en el marco de las organizaciones. Por lo tanto, el desarrollo sistemático de los procesos archivísticos comprende el conjunto de actividades organizacionales dentro de las dimensiones técnicas, administrativas, legales, tecnológicas, entre otras. De esta manera, se busca consolidar un modelo preventivo de buenas prácticas que converja con la seguridad de la información teniendo como eje estructural de análisis, al documento electrónico. Elemento que se vincula, de manera directa con instrumentos de buenas prácticas y estándares de gestión, con el objetivo de garantizar la seguridad y disposición de la información contenida en el objeto digital, en todo el proceso de desarrollo.

A continuación, se expone la figura 2 que hace referencia al Modelo Preventivo de Seguridad de Información aplicado a la Gestión de Documentos Electrónicos de carácter probatorio en las que se evidencia la aplicabilidad del instrumento MODE en convergencia con mecanismos de seguridad que contribuyen a la creación del presente modelo.

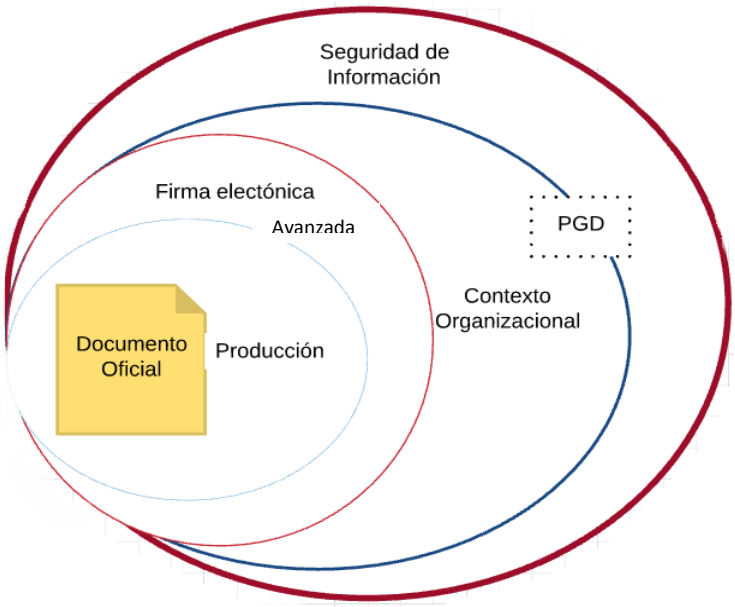

Figura 2. Modelo preventivo del documento electrónico en correlación con los procesos de gestión documental y la seguridad de información. Fuente: Elaboración propia. (2017).

Teniendo en cuenta la Figura No. 2 se procede a desarrollar cada etapa de análisis. Con el objetivo, de generar una aproximación terminológica y practica con todos los componentes del modelo en mención. Por consiguiente, se debe clarificar que la gestión de los documentos electrónicos tiene que incorporarse dentro de la continuidad del negocio e identificarse como esencia de los sistemas dentro del marco de las organizaciones.

Por esta razón, se define una serie de etapas teniendo como base el Programa de Gestión Documental del Archivo General de la Nación, en el que el documento electrónico se vincula desde su etapa de creación, lo cual implica abordar una transición que desarrolle de manera secuencial las actividades y procesos de la gestión de los documentos electrónicos. Resultado de un marco unificador de la archivística con la seguridad informática, gracias a la aplicación de un modelo basado en características externas e internas del documento, en función de un instrumento que garantice su gobernabilidad e identidad a nivel organizacional.

Llegados a este punto, se procede analizar al documento electrónico, desde el momento en que se vuelve oficial en la capa de negocio. Para entender mejor esto, se contextualizara en cada etapa del Programa de Gestión Documental (PGD) y de manera secuencial se asociara a los Metadatos Obligatorios para el Documento Electrónico (MODE) como primer instrumento enfocado en garantizar la seguridad y continuidad de la información, es decir, que será accesible en el tiempo, permitiendo corroborar su valor probatorio.

4.2.1. Fase de producción

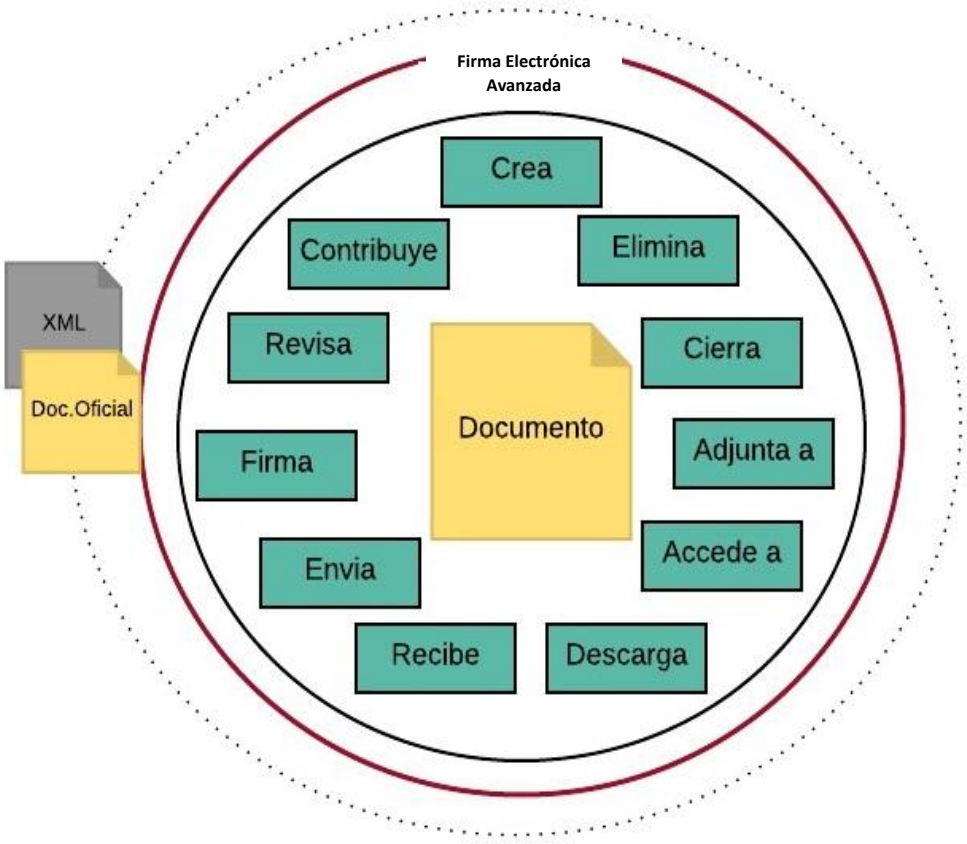

Figura 3. Procesos aleatorios de la producción de un documento oficial. Fuente: Elaboración propia. (2017).

En relación a la figura No.3 en esta fase, la organización debe determinar de manera aleatoria las actividades que se desarrollan en el momento en el que uno documento se vuelve oficial dentro sus procesos organizacionales. Lo cual, implica que se establezca una regla de negocio, en la que se opte por una adecuada gestión de los documentos desde la relación interdisciplinar con sus actividades cotidianas. De esta manera, se propone una aproximación metodológica en la etapa de producción del documento, en el que se asocia con el esquema de metadatos mínimos obligatorios del documento electrónico, anteriormente expuestos. Todo esto, para establecer requerimientos que disminuyan riesgos

operativos, administrativos y de seguridad dentro de las etapas en las que el documento es oficial dentro de los procesos de la entidad.

La organización debe contar con una certificación de la Norma Técnica Colombiana ISO 27000 enfocada en los sistemas de la gestión de seguridad de la información (SGSI) para llevar acabo los próximos instrumentos que se harán mención en el presente modelo.

Por tanto, para entender los procesos documentales de una organización de manera armónica, se debe tener en cuenta la representación gráfica de la estructura de la entidad, con el objetivo de identificar las diferentes partes y funcionalidades que se desarrollan en ella y a su vez definir relaciones y divergencias. En este parámetro, se realiza una ejemplificación del organigrama de una entidad (*a*) con el objetivo, de asociar el esquema de metadatos mínimos requerido para los documentos electrónicos.

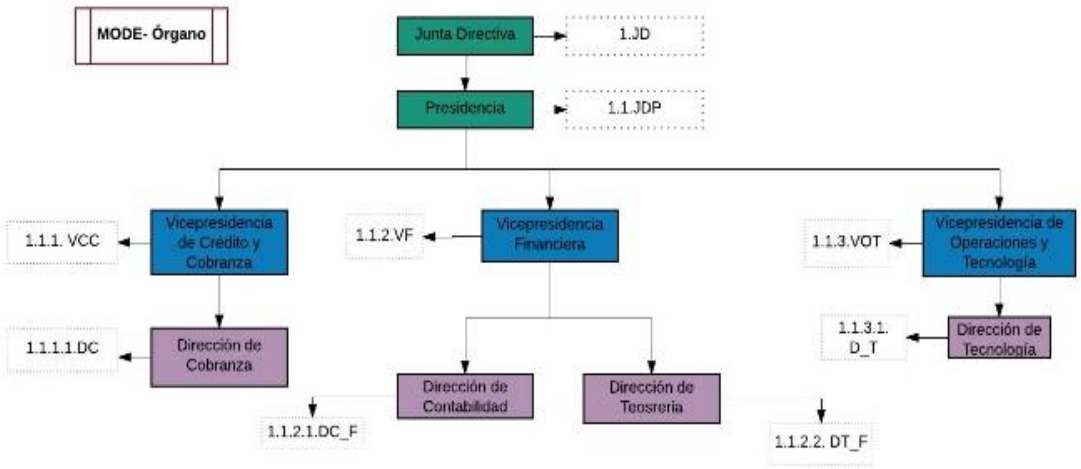

Figura No. 4. Organigrama desde la estructuración de MODE-Órgano. Fuente: Elaboración propia. (2017).

Como se evidencia, en este apartado la organización debe asignar el MODE-Órgano ya que resulta indispensable para estipular los macro procesos de la organización, en función de determinar la asignación de dependencias y relaciones existentes dentro del esquema de negocio. Para entender las

características técnicas de la asignación de este metadato, se debe proceder al diccionario de metadatos asignado en el Anexo *(a*) del presente documento. Seguido de este esto, se debe tener en cuenta la normalización de términos en las diferentes dependencias de la entidad. Debido a que, resulta crucial establecer una interoperabilidad entre los diferentes sistemas y a su vez generar una comunicación asertiva por parte de todos los agentes activos y pasivos en la unidad.

Para ejemplificar, en la figura No. 4 Se asigna una identificación alfa numérica para cada dependencia, acorde al grado de jerarquía en el que se encuentre categorizado ya que, por medio de las iniciales de cada departamento y un número consecutivo correspondiente a cada elemento y subelemento se asocia a las dependencias. Seguido de esto, se procede a realizar la asignación del Metadato MODE – Identificador donde se debe estipular un valor único de una entidad en un dominio, siendo esto, una regla de negocio fundamental para la adecuada gestión de los documentos.

A continuación se expone dos sub elementos del Metadato obligatorio Identificador, con el objetivo de ejemplificar los valores asignados para cada dependencia, acorde al organigrama antes expuesto. Por lo tanto, se busca normalizar la información para que a nivel documental en la organización se posibilite el desarrollo de un lenguaje en común dentro del marco de actuación documental y el proceder organizacional. Para asignar un identificador único se debe tener en cuenta mínimo seis (6) dígitos consecutivos, únicos e incrementales asignados para cada dependencia de la unidad. En este orden de ideas, se debe proceder a la aplicación del sub elemento MODE- secuencia de identificador teniendo en cuenta la siguiente estructura:

Ejemplo: Para la dependencia Dirección de Tesorería que hace parte de Vicepresidencia Financiera se le asigna: CO_ *1.1.2.1. DT_F_000001(*esto es, la identificación geográfica del país, seguido de la clasificación numérica asignada acorde al grado jerárquico, las siglas de la dependencia normalizadas y finalmente

seis dígitos consecutivos incrementales dentro del grado de producción documental)

Seguido de esto, se procede a realizar la vinculación con el MODE-Esquema de identificador empleado para determinar la secuencia de la entidad Documento que procede del identificador macro. Para el desarrollo del esquema se aplica la siguiente normalización:

CO_<Código dependencia><AAAA>_<ID_Único>

A continuación se procede a ejemplificar acorde a la Figura No. 3. Teniendo en cuenta la contextualización y procesos de la entidad:

CO_1.JD_2017_000001

CO_1.1.JDP_2017_000002

CO_1.1.1.VCC_2017_000003

CO_1.1.1.1.DC_2017_000004

CO_1.1.2.VF_2017_000005

CO_1.1.2.1. DC_F_2017_000006

CO_1.1.2.2. DT_F_2017_000007

CO_1.1.3.VOT_2017_000008

CO_1.1.3.1.D_T_2017_000009

CO_1.1.3.1.D_T_2017_000010

Dentro del proceso de creación del documento electrónico, la organización debe estipular en su etapa de origen el metadato MODE-Fecha de Captura, ya que, se debe asignar siempre a cualquier objeto digital. Con el objetivo, de identificar evidencia electrónica de la información registrada y determinar eventos y procesos específicos. Es importante, asignar el formato de fecha acorde a la Norma

Internacional ISO 8601:2004 donde se especifica la representación numérica asignada: (AAAA-MM-DD) – (hh:mm:ss).

Una vez realizado estos procesos de normalización, se debe tener en cuenta el ciclo de producción aleatorio expuesto anteriormente, ya que, se tiene que establecer un proceso de verificación de las características internas y externas del documento oficial. Con el objetivo, de poder constatar su validez durante largos periodos de tiempo empleando estrategias de seguridad que consoliden el intercambio de información de manera automatizable cumpliendo, con los principios de autenticidad, integridad, confiabilidad, disponibilidad y no repudio.

Por esta razón, una vez se da la producción del documento surge la obligatoriedad de consolidar una firma electrónica que garantice las propiedades del documento en el tiempo. La organización está en la obligación de establecer una política de firma que de soporte a los diferentes procesos a lo largo del ciclo de vida del documento oficial. En consecuencia, resulta indispensable, esclarecer la tipología y funcionalidad del elemento en mención que se emplea estratégicamente con el instrumento de metadatos obligatorios. Para el propósito de esta investigación se va seguir el estándar XAdES de Firma electrónica avanzada para XML.

Antes de continuar, se debe esclarecer que no se seleccionó el estándar PAdES ni CAdES ya que sus funcionalidades se engloban desde la dimensión de firma avanzada, pero no cumplen con el requerimiento estratégico de este modelo. Por lo tanto, el estándar XAdES posibilita un lenguaje entre maquinas, lo cual trae una ventaja respecto a las firmas en este tipo estructura. Debido a que, el modelo XML permite firmar varios nodos de un mismo documento. Más aún, es la tecnología que en la actualidad permite la integración de información y datos, desde la dimensión visual y esquemática, por tanto, todas las aplicaciones actuales de firmado soportan el formato XML. Lo cual, lo convierte en un agente aliado dentro de los grados de obsolescencia tecnológica y a su vez, se vuelve interoperable dentro de diferentes recursos, debido que, una firma XML, puede abarcar diferentes objetos digitales.

De acuerdo a las evoluciones del formato y los diferentes escenarios en los que se desarrolla, se propone dos tipos de firmado que hacen parte del estándar XAdES y que cumplen con los parámetros de seguridad de información desde el momento en el que el documento se vuelve oficial, dentro de la cadena de producción del presente modelo. A continuación se expone dos de las opciones que la organización puede escoger para establecer el formato de firma más preferente para sus necesidades de negocio:

- XAdES-XL (extended long-term): incorpora todos los certificados generando una validación de las fuentes respectivas, lo cual permite la verificación en el futuro, garantizando la consulta de los certificados y las listas que ya no se encuentren disponibles. –refirmado-
- XAdES-A (archivado): incorpora la modalidad de TimeStamping de manera periódica, ya que, permite asociar la políticas de refirmado una vez caduca la firma dentro del periodo de tiempo establecido por la organización. Por ejemplo, se puede emplear un periodo de un año de acuerdo al tipo de documento, estado de retención y disposición en el que se encuentre. Esta modalidad, posibilita prevenir niveles de riesgo asociados a la firma durante un periodo largo de almacenamiento.

Una vez seleccionado el formato de firma electrónica XML, se debe garantizar las propiedades de los documentos oficiales, teniendo en cuenta el ciclo de producción que garantice parámetros de seguridad desde el momento en el que el documento ha sido creado y firmado posteriormente. Todo esto, con el objetivo de vincularlo desde su etapa de producción con la NTC/ISO 27000 de seguridad de información.

4.2.2. Fase de Gestión

Para el desarrollo de esta etapa, la organización debe asegurarse de llevar el registro y vinculación de todas las actuaciones en materia de distribución de información dentro del desarrollo de sus procesos. Teniendo en cuenta, que la gestión de los documentos debe garantizar la disponibilidad, consulta y recuperación de los mismos en el sistema de información, producto de una política de trasparencia y seguridad en relación a las funciones documentales.

Por tanto, siguiendo las etapas de tiempo del presente modelo en relación al documento electrónico y su vinculación con el esquema de metadatos, como elemento instrumental del presente estudio. Se genera un periodo de transición en el que el documento debe ser revisado en materia de elaboración y seguir una categorización acorde al estado en el que se encuentra. De esta manera, la entidad debe contar con un identificador mínimo de 4 dígitos normalizado que permita especificar la asignación del metadato obligatorio MODE – Estado de elaboración como elemento estructural dentro de la cadena de producción, gestión y trazabilidad.

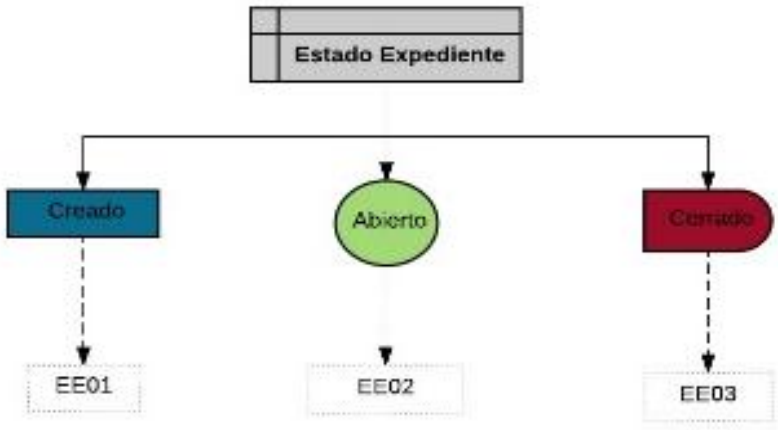

Figura No.5. Posibles estados de elaboración de un expediente electrónico. Fuente: Elaboración propia. (2017).

Como se evidencia en la Figura No.5. Los estados de elaboración de un objeto digital pueden tener una serie de variaciones de acuerdo a la producción. Por consiguiente, desde un análisis local los documentos electrónicos y en su agrupación más amplia el expediente pueden ser gestionados de diferentes maneras y tener variaciones acorde al orden de elaboración. De manera que, se vuelve indispensable implementar este metadato dentro de la cadena del objeto digital, con el objetivo, de verificar la evidencia y el valor probatorio del mismo. Por consiguiente, la asignación alfa numérica que se le asigne, debe ser secuencial, única e incremental acorde al estado en el que se encuentre.

Seguido de esto, la entidad debe establecer desde el momento en el que el documento es creado y se le atribuye el valor de oficial dentro del modelo de negocio. Proceder a la asignación inmediata de metadatos de características técnicas, que aseguren sub elementos como: formato, nombre del formato y versión del formato de esta manera se podrá contar con una trazabilidad probatoria en el sistema evidenciado las propiedades fidedignas del documento.

4.2.3. Fase de Organización del documento Oficial

Una vez realizado el proceso de identificación de los procesos iniciales en relación a la creación, gestión y trámite del documento electrónico se procede a realizar la vinculación con la fase de organización, elemento indispensable para identificar la búsqueda y recuperación de la información en las diferentes instancias. De esta manera que, la organización en el marco de sus actividades y procesos, debe establecer un esquema de tipo documental donde se asocie un código único que permita la normalización e interoperabilidad en los sistemas. Se procede a la asignación del metadato obligatorio MODE- Tipo documental.

A continuación se adjunta las diferentes tipologías documentales que se presentan en la mayoría de las organizaciones con la respectiva codificación que se le designa acorde a la sigla TD (tipología documental) y la secuencia de identificación numérica acorde a la dependencia.

Código	Tipo Documental
TD01	Acta
TD02	Acuerdo
TD03	Acuse de recibo
TD04	Alegación
TD05	Certificado
TD06	Comunicación ciudadano
TD07	Comunicación
TD08	Contrato
TD09	Convenio
TD10	Declaración
TD11	Denuncia
TD12	Diligencia
TD13	Factura
TD14	Informe
TD15	Notificación
TD16	Otros Incautos
TD17	Publicación
TD18	Recursos
TD19	Resolución
TD20	Solicitud

Tabla 5. .Tipologías documentales. Fuente: Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

No obstante, la organización debe establecer un reglamento interno para la gestión de documentos electrónicos, teniendo en cuenta la aplicación de instrumentos como:

- Cuadro de clasificación Documental (CCD)
- Tabla de Retención Documental (TRD)

Estos dos instrumentos deben llevarse acorde a lo estipulado por el Archivo General de la Nación y las normas existentes para ello. Sin embargo, el presente modelo propone el tercer instrumento que busca complementar y estructurar la visión archivística desde la relación emergente con la seguridad informática. En este caso, el esquema de metadatos como primera pauta de análisis, que se ha expuesto hasta el momento en las tres primeras etapas del Programa de Gestión Documental (PGD).

4.2.4. Vinculación de las fases de transferencia, disposición y preservación en el control de eventos

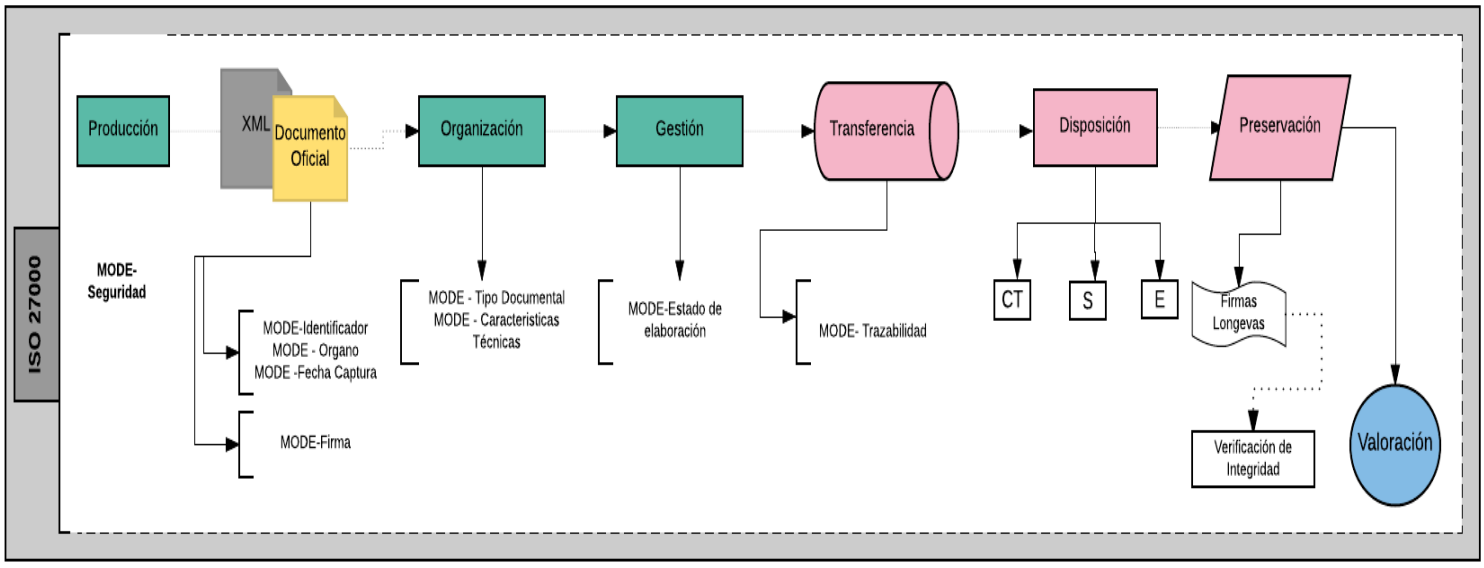

Figura No.6. Control de eventos desde el Programa de Gestión Documental y la Seguridad de Información. Fuente: Elaboración propia. (2017).

En este parámetro, se busca denotar los elementos mínimos requeridos para garantizar la creación, gestión y disposición final de un documento oficial. Así pues, se busca que las organizaciones, opten por la implementación del presente modelo para garantizar buenas prácticas en la gestión de documentos electrónicos. En primera instancia, se ha expuesto de manera secuencial las tres primeras fases de la producción documental, en la que se evidencia elementos necesarios para garantizar el correcto tratamiento de la documentación desde su etapa de creación y su posterior disposición final. Así pues, aplicando de manera relacional el Esquema de metadatos obligatorios propuesto para el documento electrónico, como instrumento de buenas prácticas, producto de la propuesta del modelo en desarrollo.

Llegado a este punto, se busca realizar una convergencia, con las fases posteriores con el objetivo, de poder oficializar un documento con características fidedignas. Por lo tanto, se procede a vincular metadatos obligatorios que resultan indispensables para las fases de: Transferencia, Disposición, Preservación y Valoración. Los cuales, resultan indispensable dentro del proceso oficialización de un documento electrónico.

Sin embargo, el objetivo del presente estudio está enmarcado en garantizar las propiedades del documento electrónico en el tiempo. Por consiguiente, las organizaciones deben integrar el Programa de Gestión Documental (PGD) con la NTC-ISO 27000 de Seguridad de Información resultado de un estudio correlacional de la ciencia archivística con la seguridad informática.

De manera que, se debe integrar estos componentes desde la etapa de creación del documento, en función de garantizar todas las propiedades. Por consiguiente, esta iniciativa busca identificar el control de eventos en el que el documento se ve involucrado. Por tanto, para las fases restantes se le asigno los metadatos MODE-

Firma y MODE-Trazabilidad. Componentes que se vinculan de manera intrínseca con la seguridad de información y finalmente, el MODE- Seguridad que a su vez presenta una categorización de sub elementos correlacionados desde la etapa de producción hasta la valoración final. Para verificar la relación con entidades, objetivos y finalidad de los metadatos empleados en esta instancia se puede puntualizar en el diccionario de datos anexado en el documento.

Seguido de esto, se debe esclarecer la funcionalidad de la firma electrónica avanzada que se aplica según el estándar XAdES se especializa en el formato XML. Este instrumento de seguridad, permitirá realizar una convergencia con los metadatos obligatorios propuestos en el modelo, ya que, el usuario podrá visualizar y editar el contenido del documento oficial, pero no podrá modificar el código fuente que se dispondrá en el archivo XML. A continuación se expone la propuesta de seguridad:

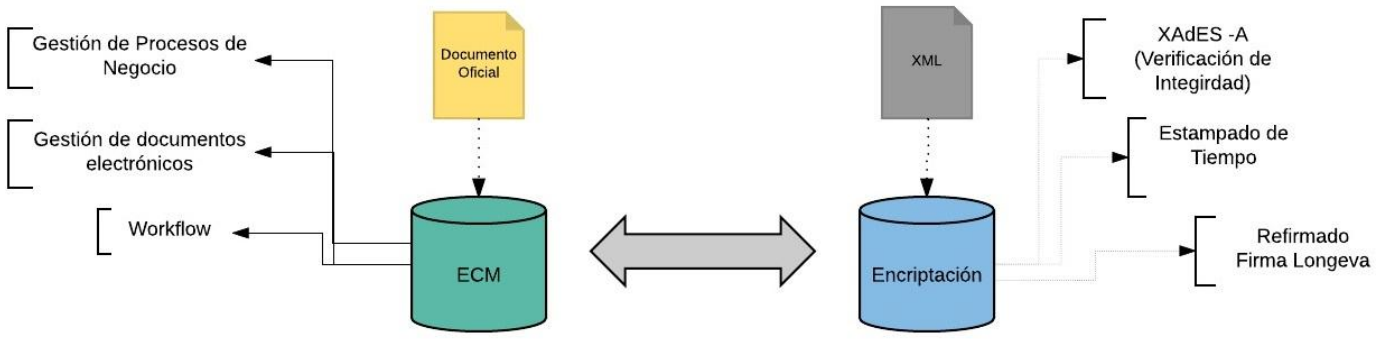

Figura No.7. Visualización y esquematización del modelo de documentos electrónicos. Fuente: Elaboración propia. (2017).

Como se evidencia en la figura No. 7 existe una independencia de repositorios que tienen por funcionalidad diferentes procesos en el contexto de negocio, teniendo como base los documentos electrónicos. Por consiguiente, se establece una correlación que permita instaurar una conexión de los servicios de la seguridad de información y la seguridad informática.

Teniendo en cuenta lo anterior, la capa de negocio permite realizar la visulización del usuario, ya que, identifica los flujos de trabajo, la gestión de los documentos electrónicos y a su vez los diferetentes procesos y resultados que se obtiene de acuerdo a su gestión. Sin embargo, los instrumentos que se han expuesto en relación a la producción del documento se han visualizado desde la ciencia archivistica (Programa de Gestión Documental) como insumo de buenas prácticas, lo cual permite la incorporación de los metadatos obligatorios para documentos electrónicos expuestos en el diccionario de datos y que presentan una correlación de tiempo con cada etapa del documento.

```
<?xml version="1.0" encoding="UTF-8"?>
<declaracion_tesoreria>
<mode_identificador>
            <mode_secuencia_identificador>CO_1.1.2.2. DT_F_2017_000007</mode_secuencia_identificador>
            <mode_esquema_identificador>1.1.2.2.DT_F_2017_000007</mode_esquema_identificador>

<mode_fecha_captura>2017-05-03</mode_fecha_captura>
            <mode_hora_captura>13:25:05</mode_hora_captura>

<mode_tipo_firma>firmalongeva</mode_tipo_firma>
    <mode_formato_firma>XAdES-A</mode_formato_firma>
    <mode_algoritmo>Hash</mode_algoritmo>
    <mode_valor>eabb08cf862daedddd5cb4cb9427938178a8dc81e127aad70f4d8954d9a3bc7bb4f2c0b24c0901f9a346dc6dc098c1f0c259230cbc2070f7e6671e4b13adfbd2</mode_valor>

<mode_estado_elaboracion>EE01</mode_estado_elaboracion>

<mode_tipo_documental>TD10</mode_tipo_documental>

<mode_caracteristicas_tecnicas>
    <mode_nombre_formato>PDF</mode_nombre_formatoformato>
    <mode_version_formato>PDF_1.7 Adobe_Extension_Level_3_Acrobat9.0</mode_version_formato>
</mode_caracteristicas_tecnicas>

<mode_trazabilidad>
      <mode_descripcion_accion>Crea</mode_descripcion_accion>
      <mode_fecha_accion>2017-05-03</mode_fecha_accion>
      <mode_hora_captura>13:25:05</mode_hora_captura>
      <mode_objeto_accion>Declaración de activos del bimestre fiscal</mode_objeto_accion>

</mode_trazabilidad>

<mode_seguridad>
       <mode_nivel_acceso>Confidencial</mode_nivel_acceso>
       <mode_nivel_confidencialidad_informacion>Medio</mode_nivel_confidencialidad_informacion>
       <mode_sensibilidad_datos_caracter_personal>Medio</mode_sensibilidad_datos_caracter_personal>
</mode_seguridad>

<verificacion_integridad>eabb08cf862daedddd5cb4cb9427938178a8dc81e127aad70f4d8954d9a3bc7bb4f2c0b24c0901f9a346dc6dc098c1f0c259230cbc2070f7e6671e4b13adfbd2</verificacion_integridad>
<sellado_tiempo>2017-05-03 T 13:25:05 UTC</sellado_tiempo>
   <archivado_sellado_tiempo>2017-05-03 T 13:25:05 UTC</archivado_sellado_tiempo>

   </declaracion_tesoreria>
```

Figura No. 8. Ejemplificación Modelo XML con verificación de integridad y sistema de firmado. Fuente: Elaboración propia. (2017).

Teniendo en cuenta la figura No.8. Se realiza una ejemplificación de un proceso dentro de la organización, el cual tiene por funcionalidad enmarcar todos los

instrumentos mencionados siendo esto, el resultado del Modelo Preventivo de Seguridad de Información aplicado a la Gestión de Documentos Electrónicos con valor probatorio. Producto de un documento desde la visualización XML, debido al estándar de implementación de seguridad de información anteriormente nombrado. Se busca converger con los instrumentos de la propuesta desde la visualización estructurada de la información y los mecanismos de actuación que permitan identificar la transparencia del documento oficial al nivel de ser gobernado por componentes holísticos en su función probatoria.

La estrategia del modelo consiste, en seguridad aplicada desde un archivo XML que tenga convergencia con los metadatos obligatorios disponibles en el diccionario de datos, anexo (a). Una vez se identifica, el momento en el que el documento se vuelve oficial en la capa de negocio, se debe asumir una convergencia de servicios que se asocien a la gestión estratégica y táctica de los procesos y procedimientos, ya que, desde los propósitos de la seguridad de información, se busca analizar, riesgos y futuras amenazas que den una consolidación del modelo. Siendo, un escenario propicio de buenas prácticas, debido a que, se busca garantizar escenarios de construcción de seguridad que asegure los procesos tecnológicos, y la producción del objeto digital hasta su estado de disposición final.

De esta manera, una vez se articula desde la seguridad de la información, se procede a realizar la implementación entorno a la protección de la información y la categorización de tecnologías, que resultan indispensables para el control de eventos, de manera que, permite evidenciar una rastreabilidad de anomalías, incidentes y detección de sucesos que puedan alterar la gobernanza organizacional en materia de transparencia y acceso a la información, siendo producto de la seguridad informática como disciplina de aplicación.

Lo cual, permitirá dejar rastreabilidad de los procesos en los que el documento se ha visto embebido. Por lo tanto, se evidenciara un control de eventos secuenciales en los que se certificara una periodicidad con el sistema de firmado a partir de

los procesos que se han desarrollado teniendo en cuenta una validación con el sellado de tiempo. Como consecuencia, se propone un insumo de buenas practicas que posibilite un sistema de firma longeva con caracteristicas de un sistema de archivado, garantizando las propiedades del documento, a partir de la verificación de integridad, que actua deacuerdo al estandar empleado como un sistema de refirmado de acuerdo a la validación que se otorga con el sellado de tiempo. Teniendo como resultado, un repositorio controlado que gira entorno a la gestión del documento electrónico de manera correlacional empleando capas de seguridad cada vez más robustas.

La organización debe interpretar de manera rigurosa los mecanismos de seguridad de información, ya que, la asignación de la etiqueta de verificación de integridad podrá certificar si el documento ha sido alterado en algún componente de su estructura. Los resultados se evidenciaran en la corroboración del HASH, que otorga una codificación del documento en función de verificar que no ha sido alterado.

El desarrollo de este modelo articulado con la norma de seguridad de información y los componentes instrumentales expuestos, debe garantizar una cultura de seguridad de información en la organización. Por consiguiente, la aplicación de auditorías internas ayudara a determinar controles conforme a los procesos y procedimientos que ha seguido la unidad, debido a la responsabilidad que se asigna por parte de la ISO 27000 para definir y planificar acciones de mejora continua en relación a los resultados obtenidos a partir de la estructuración de los registros de auditoria. Teniendo en cuenta, la gestión de incidentes, política y organización de la seguridad de información desde la evaluación de riesgos que propone el estándar normativo. De esta manera, permitirá constatar procesos futuros que la organización requiera entorno a la implementación de una cadena de custodia en relación a la evidencia digital reflejo de un protocolo integro que responde a la transparencia de la entidad y el valor probatorio del documento.

Una vez se establezcan estos protocolos a nivel organizacional, se dispone a entregar el documento al sistema de seguridad de información que actúa como capa universal de todos los procesos, funciones, actividades y protocolos expuestos en el desarrollo de este modelo. Por lo cual, es indispensable gozar con una certificación en la NTC/ISO 27000 para que verifique la normalización y el correcto cumplimiento desde la etapa inicial hasta la disposición final del documento, generando una convergencia global con la ciencia archivista y la seguridad informática. Se debe comprender que lo establecido por la norma se ajuste con las necesidades de la organización teniendo en cuenta el Sistema de Gestión de Seguridad de Información (SGSI). Se debe establecer una independencia de capas acorde a la gestión de tareas, esquemas y directrices de seguridad que se conecten por servicios en consonancia con las propiedades de la norma. Debido a que, se esclarece que la organización instaurara, operara, implementara y llevara el control adecuado acorde al contexto organizacional. Teniendo en cuenta, el establecimiento de responsabilidades que proveerá evidencia de los resultados desarrollados dentro del proceso de mejora del Sistema de Gestión de Seguridad de Información.

Componentes íntegramente relacionales que buscan gozar dentro de su esquema de negocio, con documentos fidedignos que garanticen sus propiedades a lo largo del tiempo y de esta manera disminuir los diferentes delitos de seguridad de información que atentan con la disponibilidad de un documento original. Por consiguiente, una vez el documento nace, se adquiere su equivalente de seguridad que converge en todo el ciclo de vida, otorgando una validación en el tiempo, que certifica las propiedades de integridad, autenticidad, confiabilidad, no repudio y disponibilidad.

CAPÍTULO V

5. Conclusiones

A través de esta investigación, se exploraron diferentes postulados y teorías sobre la ciencia archivística, la seguridad informática y el proceder jurídico entorno a los documentos electrónicos de archivo. Se encontraron aportes significativos que posibilitaron una orientación hacia la construcción teórica y metodología de la presente investigación.

- Las organizaciones colombianas certificadas en la ISO 27000 caso de estudio de este trabajo, presentan una particularidad entorno a su capa tecnológica debido a la implementación de la norma. Posibilita la incorporación estratégica de mecanismos de seguridad de información entiéndase desde la incorporación de los instrumentos MODE, El estándar firma electrónica avanzada, la incorporación del estándar XML y buenas prácticas en función de garantizar la seguridad, que se articulen de manera armónica con los documentos electrónicos objeto de estudio del presente modelo.
- Las organizaciones deben dimensionar la seguridad de información desde el primer momento en el que el documento se vuelve oficial en la capa de negocio. De esta manera, se contemplara protocolos de transparencia,

acceso y disponibilidad de los objetos digitales con el objetivo de velar por sus propiedades fidedignas teniendo como resultado documentos con valor probatorio.

- Una vez se establece un documento oficial dentro de la capa de negocio se debe identificar la trazabilidad documental que permita verificar el valor probatorio, las políticas de seguridad de información y la gobernanza documental. Siendo elementos íntegramente relacionados en cualquier esquema de negocio transparente.

- La implementación estratégica del esquema de metadatos, el estándar de firma longeva y la disposición de la capa de seguridad de información por la norma ISO 27000 permitió consolidar la creación de un modelo preventivo que garantiza las propiedades fidedignas del documento electrónico de archivo entiéndase: autenticidad, integridad, disponibilidad, no repudio y confiabilidad. Elementos que se consolidan como resultado de un modelo que garantiza políticas y procedimientos en función de mecanismos de defensa, en favor del documento todo el ciclo de vida, siendo el tiempo elemento estratégico. Por lo tanto, es indispensable que la entidad goce con una cultura de seguridad de información entorno al proceder documental.

- La identificación del control de eventos permitirá integrar disciplinas que se correlacionan sobre la naturaleza y trazabilidad del documento en el tiempo. Entiéndase desde la dimensión archivística, jurídica e informática. Por lo tanto, las entidades colombianas deben asegurarse, que tanto el sistema de gestión de documentos electrónicos y la capa de seguridad informática están asociadas a políticas y procedimientos de seguridad, entorno a buenas prácticas ya que, cualquier vacío podrá ocasionar riesgos enfocados ataques informáticos, que afecten con las propiedades del documento electrónico.

5.1. Recomendaciones

- Es importante explorar en terrenos que no solo converjan en la visión del archivística, sino dimensionar desde una ciencia interdisciplinar que posibilite una consolidación heurística ante posibles estudios. Como diría el filósofo de la administración del siglo XX Peter Drucker “la mejor forma de predecir el futuro es crearlo” por tanto, el presente estudio deja líneas de investigación futuras ya sea desde la informática, la evidencia digital, la ciencia jurídica y el proceder documental para realizar nuevos aportes teóricos entorno al objeto de estudio.
- Existen diferentes instrumentos y técnicas para describir el contexto y la funcionalidad de los documentos electrónicos. Sin embargo, las organizaciones no se deben limitar a la implementación de elementos básicos. Por el contrario, se debe consolidar una estructura de seguridad cada vez más robusta que disminuya riesgos operativos, administrativos, tecnológicos, entre otros.

REFERENCIAS BIBLIOGRÁFICAS

Acuerdo No. 05. Archivo General de la Nación. Por el cual se establecen criterios básicos para la clasificación, ordenación y descripción de los archivos en las entidades públicas y privadas que cumplen funciones públicas y se dictan otras disposiciones. Recuperado de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/ACUERDO_05_DE_2013.pdf

Acuerdo No. 060. *Por el cual se establecen pautas para la administración de las comunicaciones oficiales en las entidades públicas y las privadas que cumplen funciones públicas.* 30 de octubre 2001. Recuperado de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/ACUERDO_60_de_2001.pdf

Archivo General de la Nación. (2014). *Manual de Implementación de un Programa de Gestión Documental – PGD.* Recuperado de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/SINAE/Productos%20SINAE%202013/PGD2.pdf

BERMÚDEZ, M. (s.f). La diplomática y el documento electrónico. Recuperado de http://www.archivonacional.go.cr/pdf/diplomatica_%20documento_electronico.pdf

Bernal, C. (2006). Metodología de la investigación. México: McGraw-Hill. Recuperado de https://books.google.com.co/books?id=h4X_eFai59oC&printsec=frontcover&hl=es#v=onepage&q&f=false

Cano, J. (s.f). Introducción a la informática forense, 65-73. Recuperado de http://52.0.140.184/typo43/fileadmin/Revista_96/dos.pdf

CANO, J.J. Computación forense descubriendo los rastros informáticos. México, Alfa omega Grupo Editor, S.A

Caracol Radio. (2017, 02 de julio). Las irregularidades que investiga la Fiscalía en el caso Baco Agrario – Navelena. *Caracol Radio*. Recuperado de http://caracol.com.co/radio/2017/02/07/judicial/1486495481_934468.html

Código de Procedimiento Civil Colombiano. (1970). Decretos números 1400 y 2019 de 1970. Recuperado de http://www.cancilleria.gov.co/sites/default/files/tramites_servicios/apostilla_legalizacion/archivos/codigo_procedimiento_civil.pdf

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. (2001). *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho* interno. (Artículo 2). Recuperado de http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf

Corte Suprema de Justicia. (2014). *SP14623-2014.* Recuperado de http://www.legismovil.com/BancoMedios/Archivos/sent-sp-14623(3428)-14.pdf

Cruz, J.R. (2003). La gestión de los documentos electrónicos como función archivística. *Boletín de la Asociación Asturiana de Bibliotecarios, Archiveros, Documentalistas y Museólogos, 14 (2), 4-10.* Recuperado de https://aabadom.files.wordpress.com/2009/10/75_0.pdf

Cruz, J.R. (2009). La gestión de los documentos electrónicos como función archivística. Revista del Archivo Nacional. 73(1-12), 29-56. Recuperado de http://www.archivonacional.go.cr/pdf/articulos_ran/cruz%20mundet%20la%20gestion%20de%20los%20documentos_ran_2009.pdf

CRUZ, J.R. (2012). Archivística. Gestión de documentos y administración de archivos. Madrid, Alianza Editorial.

Decreto 2364 de 2012 (2012). Presidencia de la República de Colombia. 22, 11, 2012. Recuperado de http://wsp.presidencia.gov.co/Normativa/Decretos/2012/Documents/NOVIEMBRE/22/DECRETO%202364%20DEL%2022%20DE%20NOVIEMBRE%20DE%202012.pdf

El Tiempo. (2015, 24 de agosto). Sepa qué hacer si le roban su identidad para sacar créditos. *El Tiempo*. Recuperado de http://www.eltiempo.com/politica/justicia/suplantacion-de-identidad-en-colombia/16277087

Forte, N. (2017). Medium. *Documentos fidedignos en la transformación digital.* Recuperado de https://medium.com/@naniforte/documentos-fidedignos-en-la-transformaci%C3%B3n-digital-55a2b7dde092

Fuster, F. (1999). Archivística, archivo, documento de archivo... necesidad de clarificar los conceptos. *Anales de Documentación, 2* (2) ,103-120. Recuperado de http://revistas.um.es/analesdoc/article/view/2631/2611

Hernández, J., y González, A., y Ramos, B. (2008). Computer Security Lab. *Repudio de firmas electrónicas en infraestructuras de Calve Pública, 1-12.* Recuperado de http://www.seg.inf.uc3m.es/papers/2008recsi3.pdf

Hernández, S. (1998). Metodología de la investigación. México: McGraw-Hill. Recuperado de goo.gl/vWYBaL

HORTON F.W. Information Resources Management: Concept and Cases. Ohio: Association of Systems Management, 1979.

Ley 527. (1999). *Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.* 1999, 18, Agosto. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

Ley 564 de 2012. Código General del Proceso. Congreso de la República. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012.html

Ley 599 de 2000. Congreso de la República. Por la cual se expide el Código Penal. Recuperado de www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/Codigo_Penal_L-599-00.htm

Ley 906 de 2004. Código de Procedimiento Penal Colombiano. Congreso de la República. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=14787

Ley de Transparencia y Derecho Acceso a la Información Pública y Nacional 1712. (2014). *Presidencia de la República de Colombia.* 06, 03, 2014. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882

Ley General de Archivos 594 *Artículo 3* (2000). Ley 594 de 2000 Por medio del cual se dicta la Ley General de Archivos y se dicta otras disposiciones, 2000, 14, 07. Recuperado de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_594_DE_2000.pdf

Ley Modelo sobre Firmas Electrónicas (2001). Diario oficial núm. L13 de 19-01-2000, pp.12-20. Recuperado de http://www.unicitral.org/sp-index.htm

Mastropierro, M.C. *Diccionario de archivística en español con un anexo multilingüe y cuadros de fuentes de las entradas terminológicas.* Bueno Aires, Argentina: Alfagrama Ediciones.

Norma técnica colombiana NTC 5411-1. () Tecnología de la información. Técnicas de seguridad. Gestión de (revisar cita) la seguridad de la tecnología de la información y las comunicaciones.

Norma técnica colombiana NTC- ISO/IEC 27001. (2006). Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Recuperado de http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Norma técnica colombiana NTC-ISO/IEC 27002. (2007). Tecnología de la información. Técnicas de Seguridad. Código de práctica para la Gestión de la Seguridad de Información.

Peña, D. (2015). *De la firma manuscrita a las firmas electrónica y digital.* Bogotá, Colombia: Universidad Externado de Colombia.

Real Academia de la Lengua Española. (2017). *Diccionario de la Real Academia de la Lengua Española*. Madrid- España. Recuperado de

Registraduria Nacional del Estado Civil. (2012). *El Registro Civil Base de la Identificación. 1 de Octubre de 2012*. Recuperado de http://www.registraduria.gov.co/1-de-octubre-de-2012-No-68-El.html

Robles, M. (2015). La escritura y la firma manuscrita como elementos coadyuvantes de la seguridad documental. (Tesis Doctoral). Recuperado de http://www.tdx.cat/bitstream/handle/10803/315287/marl.pdf?sequence=1

Rodríguez Adrados, Antonio, «El Documento Negocial Informático», en Notariado y Contratación Electrónica, pp. 353 y siguientes (a) y, «La Firma electrónica», también en Notariado y Contratación Electrónica», Consejo General del Notariado, Madrid, 2000, pp. 375 http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122002000200012#42

ANEXOS

Anexo A- DICCIONARIO DE DATOS

Descripción Metadato MODE 1 – Identificador

MODE1 – IDENTIFICADOR			
Nombre oficial	MODE1 – Identificador		
Sub- elemento de	No aplica.		
Definición	Asignación única a una entidad		
Aplicabilidad	Todas las entidades		
Obligación	Obligatorio – Documento electrónico		
Automatizable	✓	**Repetible**	No aplica
Sub- Categorías	MODE 1.1. Secuencia del identificador MODE 1.2. Esquema de identificador		
Valores	Esquema		
	Valor genérico		
Compatibilidad	ISO 23081	Identificación del elemento.	
Finalidad	✓ Identificar de manera transparente la asignación de la entidad, dentro de un dominio determinado. ✓ Lograr la recuperación de entidades por medio de la asignación del elemento. ✓ Elemento estratégico para la creación de asociaciones y relaciones con otras entidades.		

Tabla 6. Descripción Metadato MODE 1 – Identificador. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE 1.1. – Secuencia Identificador

MODE1.1 – SECUENCIA IDENTIFICADOR	
Nombre oficial	MODE 1.1. – Identificador –Secuencia de Identificador
Sub- elemento de	MODE 1 – Identificador

Definición	Caracteres que identifican la relación de una entidad en una escala global – local.		
Aplicabilidad	Todas las entidades		
Obligación	Obligatorio – Documento electrónico		
Automatizable	✓	**Repetible**	No aplica
Sub- Categorías	No aplica.		
Valores	Esquema		Sin definir
	Valor genérico		Sin definir
Compatibilidad	ISO 23081		Identificación del elemento.
Finalidad	✓ Identificar la secuencia de la entidad (es) dentro de un determinado campo.		

Tabla 7. Descripción Metadato MODE 1.1. – Secuencia Identificador. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE 1.2. – Esquema de Identificador

MODE1.2. – ESQUEMA DE IDENTIFICADOR			
Nombre oficial	MODE 1.2. – Identificador –Esquema de Identificador		
Sub- elemento de	MODE 1 - Identificador		
Definición	Esquema que busca crear la relación secuencial de los diferentes caracteres dentro de las entidades.		
Aplicabilidad	Todas las entidades		
Obligación	Condicional – Aplicación acorde a la asignación de un identificador a una entidad de acuerdo al contexto desarrollo.		
Automatizable	✓	**Repetible**	No aplica
Sub- Categorías	No aplica.		
Valores	Esquema		Sin definir
	Valor genérico		Sin definir
Compatibilidad	ISO 23081		Identificación del elemento.
Finalidad	✓ Esquema que procede del identificador para establecer sus diferentes relaciones.		

Tabla 8. Descripción Metadato MODE 1.2. – Esquema de Identificador. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.2 – Órgano.

MODE 2. – ÓRGANO			
Nombre oficial	MODE 2. –Órgano		
Sub- elemento de	No aplica.		
Definición	Permite identificar la normalización que se realiza acorde a la Norma técnica de interoperabilidad aplicada a los documentos electrónicos.		
Aplicabilidad	Documento.		
Obligación	Obligatorio– Documento electrónico.		
Automatizable	✓	**Repetible**	✓
Sub- Categorías	No aplica.		
Valores	Esquema	Códigos procedentes establecidos por la organización.	
	Valor genérico	Sin definir	
Compatibilidad	ISO 23081	-	
Finalidad	Identificar el órgano que crea, captura, y es responsable del documento.		

Tabla 8. Descripción Metadato MODE.2 – Órgano. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.3 –Fecha de Captura

MODE 3. – FECHA DE CAPTURA	
Nombre oficial	MODE 3. – Fecha de Captura
Sub- elemento de	No aplica.
Definición	Identificación de la fecha asociada a un evento que se ha efectuado en una o varias entidades.
Aplicabilidad	Todas las entidades.

Obligación	Obligatorio– Documento electrónico.		
Automatizable	✓	**Repetible**	✓
Sub- Categorías	MODE 4.1. –Fecha inicio MODE 4.2. –Fecha fin		
Valores	Esquema		No aplica
	Valor genérico		No aplica
Compatibilidad	ISO 23081		-No se evidencia en la normativa, pero cumple con la funcionalidad.
Finalidad	✓ Registrar la fecha de creación y finalización de una entidad permitiendo la creación de asociaciones a nivel global dentro del organismo. ✓ Evidencia electrónica de la autenticidad de un documento. ✓ Permite evidenciar la trazabilidad y procedencia de los documentos electrónicos, en función de constatar que el documento no ha sido alterado y que goza del principio de integridad.		

Tabla 10. Descripción Metadato MODE.3 –Fecha de Captura. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.3.1. –Fecha Inicio.

MODE 4.1. – FECHA INICIO			
Nombre oficial	MODE 4.1. – Fecha de Captura- Fecha Inicio		
Sub- elemento de	MODE 4. Fecha de Captura		
Definición	Fecha en la que la entidad ha sido creada.		
Aplicabilidad	Todas las entidades.		
Obligación	Obligatorio– Documento electrónico.		
Automatizable	✓	**Repetible**	
Sub- Categorías	No aplica.		
Valores	Esquema		[<AAAA-MMDD>T<hh:mm:ss>][6]

[6] Formato de asignación de fecha y hora acorde a la Norma Internacional ISO 8601:2004

	Valor genérico	No aplica
Compatibilidad	ISO 23081	Descripción
	ISO 8601: 2004	Representaciones fecha y hora.
Finalidad	✓ Evidencia de la autenticidad del documento acorde a su fecha de creación. ✓ Creación de la relación del documento con otras entidades.	

Tabla 11. Descripción Metadato MODE.3.1. –Fecha Inicio. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.3.2. –Fecha Fin.

MODE 3.2. – FECHA FIN			
Nombre oficial	MODE 3.2. – Fecha de Captura- Fecha fin		
Sub- elemento de	MODE 3. Fecha de Captura		
Definición	Fecha en la que finaliza la creación de una entidad o ha sido transferida o eliminada.		
Aplicabilidad	Todas las entidades.		
Obligación	Condicional- Se debe aplicar solo si la entidad ha finalizado su proceso de creación o ha sido transferida o eliminada en lo relacionado a la entidad documento.		
Automatizable	✓	**Repetible**	
Sub- Categorías	No aplica.		
Valores	Esquema		[<AAAA-MMDD>T<hh:mm:ss>][7]
	Valor genérico		No aplica
Compatibilidad	ISO 23081		Descripción
	ISO 8601: 2004		Representaciones fecha y hora.
Finalidad	✓ Proporciona evidencia de la autenticidad, acorde a la fecha en que finalizo una entidad particularmente el documento. ✓ Creación de la relación fechas - finalización con		

[7] Formato de asignación de fecha y hora acorde a la Norma Internacional ISO 8601:2004

	otras entidades.

Tabla 12. Descripción Metadato MODE.3.2. –Fecha Fin. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.4. –Estado de elaboración.

MODE 4. – ESTADO DE ELABORACIÓN		
Nombre oficial	MODE 4. –Estado de elaboración	
Sub- elemento de	No aplica.	
Definición	Identifica las características de creación del documento en función de establecer si es original o posee una variedad de copias, producto del auténtico.	
Aplicabilidad	Documento Simple	
Obligación	Obligatorio –Documento electrónico	
Automatizable	✓ **Repetible**	
Sub- Categorías	No aplica.	
Valores	Esquema	EE01 (Original) EE02 (Copia electrónica autentica con cambio de formato) EE03 (Copia electrónica autentica al documento en papel)
	Valor genérico	No aplica
Compatibilidad	ISO 23081	Uso
Finalidad	✓ Identificar el grado de la elaboración del documento con el objetivo de corroborar, la evidencia de actividades y procesos en función de su valor probatorio.	

Tabla 13. Descripción Metadato MODE.4. –Estado de elaboración. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.5. –Características Técnicas

MODE 5. – CARACTERÍSTICAS TÉCNICAS			
Nombre oficial	MODE 5. –Características técnicas		
Sub- elemento de	No aplica.		
Definición	Características técnicas, lógicas y funcionales de los objetos digitales en mención.		
Aplicabilidad	Documento		
Obligación	Obligatorio –Documento electrónico		
Automatizable	✓	**Repetible**	
Sub- Categorías	MODE 5.1. – Formato MODE 5.1.1. – Nombre de Formato MODE 5.2. – Versión Formato		
Valores	Esquema	No aplica	
	Valor genérico	No aplica	
Compatibilidad	ISO 23081	Uso	
Finalidad	✓ Proporcionar información acerca de las condicione lógicas y funcionales de las diferentes características técnicas que el documento posee en el tiempo. ✓ Permitir la recuperación de los documentos acorde a una adecuada normalización de formatos. ✓ Facilitar los procesos de transferencia de la documentación acorde a las versiones y soportes en los que se encuentra la información. ✓ Garantizar la autenticidad y el no repudio de los documentos electrónicos.		

Tabla 14. Descripción Metadato MODE.5. –Características Técnicas. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.5.1. –Formato

MODE 5. 1. – FORMATO		
Nombre oficial	MODE 5.1. –Características técnicas – Formato	
Sub- elemento de	MODE 5. – Características técnicas	
Definición	Asignación lógica del formato de fichero para el documento electrónico.	
Aplicabilidad	Documento	
Obligación	Obligatorio –Documento electrónico	
Automatizable	✓ **Repetible**	
Sub- Categorías	MODE 7.1.1. – Nombre de Formato	
Valores	Esquema	No aplica
	Valor genérico	No aplica
Compatibilidad	ISO 23081	Sin compatibilidad-
Finalidad	✓ Facilitar la búsqueda de los documentos acorde a un formato específico. ✓ Ayudar a la conservación, migración y almacenamiento de los contenidos. ✓ Lograr una adecuada migración del objeto digital en mención para optimizar los procesos en el tiempo, reduciendo la obsolescencia tecnológica y la perdida de contenidos.	

Tabla 15. Descripción Metadato MODE.5.1. –Formato. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.5.1.1. – Nombre de Formato

MODE 5. 1.1. –NOMBRE DE FORMATO	
Nombre oficial	MODE 5.1. 1 –Características técnicas – Nombre de formato
Sub- elemento de	MODE 5. – Características técnicas
Definición	Asignación lógica del formato de fichero para el

	documento electrónico.		
Aplicabilidad	Documento		
Obligación	Obligatorio –Documento electrónico		
Automatizable	✓	**Repetible**	
Sub- Categorías	MODE 7.1.1. – Nombre de Formato		
Valores	Esquema		PDF-PDF/A Strict Open XML ISO / IEC 26300: 2006
	Valor genérico		No aplica
Compatibilidad	ISO 23081		Sin compatibilidad-
Finalidad	✓ Facilitar la búsqueda de los documentos acorde a un formato específico. ✓ Ayudar a la conservación, migración y almacenamiento de los contenidos. ✓ Lograr una adecuada migración del objeto digital en mención para optimizar los procesos en el tiempo, reduciendo la obsolescencia tecnológica y la perdida de contenidos.		

Tabla 16. Descripción Metadato MODE 5.1.1. – Nombre de Formato. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.5.2. – Versión Formato

MODE 5. 2. – VERSIÓN FORMATO			
Nombre oficial	MODE 5.2. –Características técnicas – Versión formato		
Sub- elemento de	MODE 5 – Características técnicas		
Definición	Versión lógica del formato de fichero para el documento electrónico.		
Aplicabilidad	Documento		
Obligación	Obligatorio –Documento electrónico		
Automatizable	✓	**Repetible**	
Sub- Categorías	MODE 7.1.1. – Nombre de Formato		
Valores	Esquema		PDF XHTML JSON
	Valor genérico		No aplica
Compatibilidad	ISO 23081		Sin compatibilidad-
Finalidad	✓ Facilitar la búsqueda de los documentos acorde a un formato específico. ✓ Ayudar a la conservación, migración y		

	almacenamiento de los contenidos. ✓ Lograr una adecuada migración del objeto digital en mención para optimizar los procesos en el tiempo, reduciendo la obsolescencia tecnológica y la perdida de contenidos.

Tabla 17. Descripción Metadato MODE.5.2. – Versión Formato. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.6. – Tipo Documental

MODE 6.– TIPO DOCUMENTAL		
Nombre oficial	MODE 6. –Tipo Documental	
Sub- elemento de	No aplica.	
Definición	Modelo que da cuenta de la estructura que adopta el documento en función de establecer una serie de procesos y procedimientos homogéneos.	
Aplicabilidad	Documento	
Obligación	Obligatorio –Documento electrónico	
Automatizable	✓ **Repetible**	
Sub- Categorías	MODE 7.1.1. – Nombre de Formato	
Valores	Esquema	Ver Apéndice 1.
	Valor genérico	No aplica
Compatibilidad	ISO 23081	Identificación no aparece en la normativa pero cumple con la funcionalidad.
Finalidad	✓ Facilitar la búsqueda y recuperación de la documentación. ✓ Mejorar la interpretación de la documentación en función de las relaciones.	

Tabla 18. Descripción Metadato MODE.6. – Tipo Documental. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.7. – Firma

MODE 7.– FIRMA			
Nombre oficial	MODE 7. –Firma		
Sub- elemento de	No aplica.		
Definición	Método que se centra en fijar las condiciones y requerimientos de autenticidad y fiabilidad al documento.		
Aplicabilidad	Documento		
Obligación	Obligatorio –Documento electrónico		
Automatizable		**Repetible**	✓
Sub- Categorías	MODE 7.1. - Tipo de firma MODE 7.1.1. – Formato de firma MODE 7.1.1.1. – Perfil de firma MODE 7.2. – Valor del CSV MODE 7.3. – Definición de Generación CSV		
Valores	Esquema		No aplica
	Valor genérico		No aplica
Compatibilidad	ISO 23081		Uso
Finalidad	✓ Determinar si el documento cuenta con las propiedades de autenticidad, fiabilidad e integridad. Teniendo en cuenta, el momento de su creación mediante una validación tecnológica empleado acciones jurídicas que vinculen a una persona natural. ✓ Capturar y encapsular las propiedades de un documento en el tiempo con el objetivo, de garantizar la autenticada, integridad y fiabilidad en el tiempo. De su creación y proceso de tiempo.		

Tabla 19. Descripción Metadato MODE.7. – Firma. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.7.1. – Tipo de Firma

MODE 7.1– TIPO DE FIRMA		
Nombre oficial	MODE 7.1 –Firma- Tipo de firma	
Sub- elemento de	MODE 7. – Firma	
Definición	Asignación normalizada del formato de firma a emplear.	
Aplicabilidad	Documento	
Obligación	Obligatorio –Documento electrónico	
Automatizable	✓ **Repetible**	
Sub- Categorías	MODE 7.1.1. – Formato de firma MODE 7.1.2. – Perfil de firma	
Valores	Esquema	Firma electrónica Firmas Longevas
	Valor genérico	No aplica
Compatibilidad	ISO 23081	Sin compatibilidad.
Finalidad	✓ Señalar el tipo de firma electrónica empleada para la seguridad de las propiedades del documento electrónico en el tiempo.	

Tabla 20. Descripción Metadato MODE.7.1. – Tipo de Firma. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016)

Descripción Metadato MODE.7.1.1. – Formato de Firma

MODE 7.1.1.– FORMATO DE FIRMA		
Nombre oficial	MODE 7.1.1. –Firma- Tipo de firma – Formato de firma	
Sub- elemento de	MODE 7. 1– Tipo de Firma	
Definición	Asignación normalizada del formato de firma a emplear.	
Aplicabilidad	Documento	
Obligación	Obligatorio –Documento electrónico	
Automatizable	✓ **Repetible**	
Sub- Categorías	MODE 7.1.1. – Formato de firma MODE 7.1.2. – Perfil de firma	
Valores	Esquema	XAdES CAdES PAdES
	Valor genérico	No aplica
Compatibilidad	ISO 23081	Sin compatibilidad.

Finalidad	✓ Señalar el tipo de firma electrónica empleada para la seguridad de las propiedades del documento electrónico en el tiempo.

.

Tabla 21. Descripción Metadato MODE.7.1.1. – Formato de Firma. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016)

Descripción Metadato MODE.7.1.2 – Perfil de Firma

MODE 7.1.2.– PERFIL DE FIRMA		
Nombre oficial	MODE 7.1.1. –Firma- Tipo de firma – Perfil de firma	
Sub- elemento de	MODE 7. 1– Tipo de Firma	
Definición	Perfil empleado en una firma que cuenta con un certificado electrónico.	
Aplicabilidad	Documento	
Obligación	Condicional – TF01, TF02, TF03, TF04, TF05 o TF06.	
Automatizable	✓ **Repetible**	
Sub- Categorías	No aplica	
Valores	Esquema	(Firmas electrónicas avanzadas)
	Valor genérico	No aplica
Compatibilidad	ISO 23081	Sin compatibilidad.
Finalidad	✓ La identificación de la tipología de firma son reglas empleadas para asegurar la relación entre los sistemas, producto de la interoperabilidad.	

Tabla 22. Descripción Metadato MODE. 7. 1.2 – Perfil de Firma. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016)

Descripción Metadato MODE.7.2. – Algoritmo

MODE 7.2. – Algoritmo	
Nombre oficial	MODE 7.2. Algoritmo
Sub- elemento de	No aplica.
Definición	"Método algorítmico reproducible que transforma la secuencia de caracteres que forma un Documento, en un valor de longitud fija, que representa el valor digital

	de dicho Documento. Se excluye el caso de CSV." (p.66).	
Aplicabilidad	Documento	
Obligación	Obligatorio- Documentos electrónicos que se migren y se transfieran a otro sistema o dentro de la misma unidad.	
Automatizable	✓ **Repetible**	
Sub- Categorías	No aplica.	
Valores	Esquema	No aplica.
	Valor genérico	No aplica
Compatibilidad	ISO 23081	Sin compatibilidad.
Finalidad	✓ Verificar si un documento ha sido alterada de manera inapropiada y no autorizada. ✓ Garantizar la autenticidad e integridad de los documentos electrónicos a lo largo del tiempo. ✓ Debe emplearse junto con el metadato de MODE 10.2. - VALOR con el objetivo, de calcular el algoritmo empleado.	

Tabla 23. Descripción Metadato MODE.7.2. – Algoritmo. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016

Descripción Metadato MODE.7.3. – Valor

MODE 7.3. – Valor		
Nombre oficial	MODE 7.3. Valor	
Sub- elemento de	No aplica.	
Definición	Valor real, generado por el algoritmo definido en MODE 10.1 - Algoritmo que representa el documento simple o conjunto de documentos a que hace referencia. (p.66).	
Aplicabilidad	Documento	
Obligación	Opcional.	
Automatizable	✓ **Repetible**	
Sub- Categorías	No aplica.	
Valores	Esquema	Esquema desarrollado por cada organización. (Asignación del Hash)
	Valor genérico	No aplica
Compatibilidad	ISO 23081	Sin compatibilidad.
Finalidad	✓ Verificar si un documento ha sido alterada de	

	manera inapropiada y no autorizada. ✓ Garantizar la autenticidad e integridad de los documentos electrónicos a lo largo del tiempo. ✓ Debe emplearse junto con el metadato de MODE 10.1. - ALGORITMO con el objetivo, de calcular el nombre del valor generado. (Asignación del Hash).

Tabla 24. Descripción Metadato MODE.7.3. – Valor. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016

Descripción Metadato MODE.8. – Trazabilidad.

MODE 8. – TRAZABILIDAD			
Nombre oficial	MODE 11. – Trazabilidad		
Sub- elemento de	No aplica.		
Definición	Información sobre las diferentes acciones realizadas sobre las entidades y trazabilidad de los metadatos en función de establecer las relaciones de creación, tramite acorde a protocolos establecidos.		
Aplicabilidad	Todas las entidades.		
Obligación	Obligatorio – Documento electrónico.		
Automatizable		**Repetible**	✓
Sub- Categorías	MODE 11.1.- Acción MODE 11.2. – Motivo Reglado MODE 11.3. – Usuario de la acción MODE 11.4. – Descripción MODE 11.5. – Modificación de los metadatos MODE 11.6. – Historia de cambio		
Valores	Esquema		No aplica
	Valor genérico		No aplica
Compatibilidad	ISO 23081		Historial de eventos.
Finalidad	✓ “La trazabilidad equivale a lo que se conoce como pista de auditoría de tal modo que la implantación de este elemento y sus subelementos dependerá de implantaciones específicas que deben respetar las buenas prácticas y normas técnicas relativas a seguimiento de acciones “ (p.74).		

Tabla 25. Descripción Metadato MODE.8. – Trazabilidad. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016

Descripción Metadato MODE.8.1. – Acción.

MODE 8. 1– ACCIÓN			
Nombre oficial	MODE 8.1 – Trazabilidad - Acción		
Sub- elemento de	MODE 8. – Trazabilidad		
Definición	Indicador de las acciones en los documentos y sus respectivas relaciones.		
Aplicabilidad	Todas las entidades.		
Obligación	Obligatorio – Documento electrónico.		
Automatizable		**Repetible**	✓
Sub- Categorías	MODE 8.1.1.- Descripción de la acción MODE 8.1.2. – Fecha de la acción MODE 8.1. 3. – Objeto de la acción		
Valores	Esquema		No aplica
	Valor genérico		No aplica
Compatibilidad	ISO 23081		Historial de eventos.
Finalidad	✓ Determinar el tipo de acción realizada en un periodo de tiempo determinado.		

Tabla 26. Descripción Metadato MODE.8.1. – Acción. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.11.1.1– Descripción de la acción

MODE 8.1.1. – DESCRIPCIÓN DE LA ACCIÓN			
Nombre oficial	MODE 8.1.1. – Trazabilidad - Acción – Descripción de la acción		
Sub- elemento de	MODE8.1. – Acción		
Definición	Descripción del tipo de acción realizada en el documento electrónico y las diferentes entidades.		
Aplicabilidad	Todas las entidades.		
Obligación	Obligatorio – Documento electrónico.		
Automatizable		**Repetible**	✓
Sub- Categorías	No aplica.		

Valores	Esquema	Definición por parte de la organización.
	Valor genérico	No aplica
Compatibilidad	ISO 23081	Historial de eventos.
Finalidad	✓ Determinar el tipo de acción realizada en un periodo de tiempo determinado.	

Tabla 27. Descripción Metadato MODE.8.1.1– Descripción de la acción. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.8.1.2– Fecha de la acción.

MODE 8.1.2. – FECHA DE LA ACCIÓN			
Nombre oficial	MODE 8.1.2. – Trazabilidad - Acción – Fecha de la acción		
Sub- elemento de	MODE 8.1. – Acción		
Definición	Indicador de las acciones en los documentos y sus respectivas relaciones. Una vez MODE 11.1. – Acción		
Aplicabilidad	Todas las entidades.		
Obligación	Obligatorio – Documento electrónico.		
Automatizable	✓	**Repetible**	✓
Sub- Categorías	No aplica.		
Valores	Esquema	[<AAAA-MMDD>T<hh:mm:ss>][8]	
	Valor genérico	Sin definir.	
Compatibilidad	ISO 23081	Historial de eventos.	
Finalidad	✓ Señalar en el momento en el que la acción ha sido realizada teniendo la relación con el metadato MODE 11.1. – Acción.		

[8] Formato de asignación de fecha y hora acorde a la Norma Internacional ISO 8601:2004

Tabla 28. Descripción Metadato MODE.8.1.2. – Fecha de la acción. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.8.1.3. – Objeto de la acción.

MODE 8.1.3. – OBJETO DE LA ACCIÓN			
Nombre oficial	MODE 8.1.3. – Trazabilidad - Acción – Objeto de la acción		
Sub- elemento de	MODE 8.1. – Acción		
Definición	Indicador del componente del documento y sus respectivas relaciones en el marco de las acciones señalada en el MODE 8.1.1 – Descripción de la acción		
Aplicabilidad	Todas las entidades.		
Obligación	Obligatorio – Documento electrónico.		
Automatizable	✓	**Repetible**	✓
Sub- Categorías	No aplica.		
Valores	Esquema		"Contenido del Documento, Metadatos del documento, Firmas del Documento, Documento Completo" (p.76)
	Valor genérico		Sin definir.
Compatibilidad	ISO 23081		Historial de eventos.
Finalidad	✓ Determinar el tipo de acción realizada en un periodo de tiempo determinado.		

Tabla 29. Descripción Metadato MODE.8.1.3. – Objeto de la acción. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.8.2. – Motivo Reglado.

MODE 8.2. – MOTIVO REGLADO			
Nombre oficial	MODE 8.2. – Trazabilidad - Motivo Reglado		
Sub- elemento de	MODE 8.- Trazabilidad		
Definición	Razón por la que se comete la acción en el metadato MODE 8.1 – Acción.		
Aplicabilidad	Todas las entidades.		
Obligación	Obligatorio – Documento electrónico.		
Automatizable		**Repetible**	✓
Sub- Categorías	No aplica.		

Valores	Esquema	Sin definir.
	Valor genérico	Sin definir.
Compatibilidad	ISO 23081	Historial de eventos.
Finalidad	✓ "Informar acerca de la motivación reglada por la que se ha llevado a cabo una determinada acción sobre una entidad" (p.77).	

Tabla 30. Descripción Metadato MODE.8 .2. – Motivo Reglado. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE. 8.3. – Usuario de la acción.

MODE 8.3. – USUARIO DE LA ACCIÓN			
Nombre oficial	MODE 8.3. – Trazabilidad - Usuario de la acción		
Sub- elemento de	MODE 8.- Trazabilidad		
Definición	Identificación del usuario que ha realizado la acción determinada en los metadatos MODE 8.1. Acción		
Aplicabilidad	Todas las entidades.		
Obligación	Opcional – Documento electrónico.		
Automatizable	✓	**Repetible**	✓
Sub- Categorías	No aplica.		
Valores	Esquema	Sin definir.	
	Valor genérico	Sin definir.	
Compatibilidad	ISO 23081	Historial de eventos.	
Finalidad	✓ "Mantener una pista de auditoría inalterable de las personas que ejecutan las acciones realizadas en el sistema." (p.77). ✓ "El usuario puede ser un nombre de usuario, el nombre completo de la persona que realiza o realizó la acción, la dirección IP del equipo del usuario" (p.77).		

Tabla 31. Descripción Metadato MODE.8.3. – Usuario de la acción. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.11.4. – Descripción.

MODE 8.4. – DESCRIPCIÓN			
Nombre oficial	MODE 8.4. – Trazabilidad - Descripción		
Sub- elemento de	MODE 8.- Trazabilidad		
Definición	Explicación detallada del texto libre en relación en MODE 8.1.1 Descripción de la Acción		
Aplicabilidad	Todas las entidades.		
Obligación	Condicional – Documento electrónico. Si se le atribuye el condicional de MODE 8.1.1. Descripción de la acción campo “cambia”		
Automatizable		**Repetible**	✓
Sub- Categorías	No aplica.		
Valores	Esquema	Sin definir.	
	Valor genérico	Sin definir.	
Compatibilidad	ISO 23081	Historial de eventos.	
Finalidad	✓ “Ofrecer una explicación más detallada en texto libre de la acción realizada sobre una determinada entidad” (p.78).		

Tabla 32. Descripción Metadato MODE.8.4. – Descripción. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.8.5. – Modificación de los metadatos

MODE 8.5. – MODIFICACIÓN DE LOS METADATOS			
Nombre oficial	MODE 8.5 – Trazabilidad - Modificación de los metadatos		
Sub- elemento de	MODE 8.- Trazabilidad		
Definición	“Información que registra la autoría y fecha de los posibles cambios que han sufrido los metadatos de una entidad una vez realizada la acción determinada” (p.78) Ver MODE 8.1. Acción		
Aplicabilidad	Todas las entidades.		
Obligación	Condicional – Documento electrónico. Solo se debe aplicar a los elementos que han sufrido alguna modificación en sus metadatos.		
Automatizable		**Repetible**	✓

Sub- Categorías	No aplica.	
Valores	Esquema	Sin definir.
	Valor genérico	Sin definir.
Compatibilidad	ISO 23081	Historial de eventos.
Finalidad	Permite identificar si el documento ha sido alterado. Por medio de la gestión de auditoria, para evidenciar las acciones en el sistema.	

Tabla 33. Descripción Metadato MODE.8.5. – Modificación de los metadatos. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.8.6. – Historia del Cambio.

MODE 8.6. – HISTORIA DEL CAMBIO			
Nombre oficial	MODE 8.6 – Trazabilidad - Historia del Cambio		
Sub- elemento de	MODE 8.- Trazabilidad		
Definición	Información de un metadato que ha sido modificado sobre un determinador valor para identificar el valor anterior.		
Aplicabilidad	Contexto de relación de la documentación.		
Obligación	Condicional – Documento electrónico. Solo se debe aplicar a los elementos que han sufrido alguna modificación en sus metadatos.		
Automatizable		**Repetible**	✓
Sub- Categorías	8.6.1. Nombre del elemento 8. 6.2. Valor anterior		
Valores	Esquema	Sin definir.	
	Valor genérico	Sin definir.	
Compatibilidad	ISO 23081	Historial de eventos.	
Finalidad	✓ Registrar los cambios que han sufrido los documentos a lo largo del tiempo. ✓ Mantener un historial de la trazabilidad de los documentos en función de acciones y procesos evidenciados en el sistema. ✓ Identificar las modificaciones y la creación de relaciones.		

Tabla 34. Descripción Metadato MODE.8.6. – Historia del Cambio. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.8.6.1. – Nombre del elemento

MODE 8.6.1. – NOMBRE DEL ELEMENTO			
Nombre oficial	MODE 8.6.1. – Trazabilidad - Historia del Cambio - Nombre del elemento.		
Sub- elemento de	MODE 11.6. – Historia del cambio		
Definición	"Nombre de un elemento o subelemento de metadato cuyo valor ha sufrido algún tipo de modificación" (p.79).		
Aplicabilidad	Contexto de relación de la documentación.		
Obligación	Condicional – Documento electrónico. Solo se debe aplicar a los elementos que han sufrido alguna modificación en sus metadatos.		
Automatizable	✓	**Repetible**	
Sub- Categorías	No aplica		
Valores	Esquema		Etiquetas asignadas por la organización.
	Valor genérico		Sin definir.
Compatibilidad	ISO 23081		Historial de eventos.
Finalidad	✓ "Identificar aquellos elementos o sub-elementos que han cambiado como resultado de una relación." (p.79).		

Tabla 35. Descripción Metadato MODE.8.6.1. – Nombre del elemento. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE.8.6.2. – Valor anterior

MODE 8.6.2. – VALOR ANTERIOR	
Nombre oficial	MODE 8.6.2. – Trazabilidad - Historia del Cambio - Valor anterior.
Sub- elemento de	MODE 8.6. – Historia del cambio
Definición	"Contenido anterior de un elemento o subelemento de metadato de una determinada entidad que ha sido modificado en un momento del tiempo" (p.80).
Aplicabilidad	Contexto de relación de la documentación.

Obligación	Condicional – Documento electrónico. Solo se debe aplicar a los elementos que han sufrido alguna modificación en sus metadatos.		
Automatizable	✓	**Repetible**	
Sub- Categorías	No aplica		
Valores	Esquema	Sin definir.	
	Valor genérico	Sin definir.	
Compatibilidad	ISO 23081	Historial de eventos.	
Finalidad	✓ Registrar los cambios que han sufrido los documentos a lo largo del tiempo. ✓ Mantener un historial de la trazabilidad de los documentos en función de acciones y procesos evidenciados en el sistema. ✓ Identificar las modificaciones y la creación de relaciones.		

Tabla 36. Descripción Metadato MODE.8.6.2. – Valor anterior. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE. 9. - Seguridad

MODE 9. – SEGURIDAD			
Nombre oficial	MODE 9. – Seguridad		
Sub- elemento de	No aplica		
Definición	Valores que en un esquema articulado, permite identificar medidas para proteger los documentos, información y datos dentro de un contexto que pueda sufrir cambios, destrucción y otras variantes.		
Aplicabilidad	Contexto de aplicación a todas las entidades.		
Obligación	Obligatoriedad – Documento electrónico. Se debe aplicar a los elementos desde su etapa de creación en relación al contexto de aplicación.		
Automatizable	✓	**Repetible**	✓
Sub- Categorías	MODE 9.1 – Nivel de Seguridad MODE 9.2 – Permisos MODE 9.3 – Nivel de confidencialidad de la información. MODE 9.4 – Sensibilidad de datos de carácter personal		
Valores	Esquema	No aplica.	
	Valor genérico	No aplica.	

Compatibilidad	ISO 23081- ISO 27001	Seguridad de información (Uso)
Finalidad	✓ El objetivo principal de este elemento es establecer variables que aseguren de manera rigurosa el estado interno y externo de la documentación en materia de seguridad de información. ✓ Garantizar la protección de todas las entidades en mención.	

Tabla 37. Descripción Metadato MODE.9. – Seguridad. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE. 9.1. – Nivel de Seguridad

MODE 9.1. – NIVEL DE SEGURIDAD			
Nombre oficial	MODE 9.1. – Seguridad – Nivel de Seguridad.		
Sub- elemento de	MODE 9. – Seguridad		
Definición	Determina la categoría de seguridad y riesgo de un documento o agente.		
Aplicabilidad	Contexto de aplicación a todas las entidades.		
Obligación	Condicional – “Debe utilizarse si el documento o la regulación tiene un nivel de seguridad en su jurisdicción” (p.34).		
Automatizable		**Repetible**	✓
Sub- Categorías	MODE 9.1.1. – Nivel de Acceso		
Valores	Esquema		No aplica.
	Valor genérico		No aplica.
Compatibilidad	ISO 23081- ISO 27001		Seguridad de información (Uso)
Finalidad	✓ Determinar criterios de seguridad para los documentos con el objetivo de protegerlos adecuadamente. ✓ “Facilitar o restringir el acceso a los documentos, o a funciones, actividades o actuaciones particulares, por agentes como el personal de la organización” (p.34)		

Tabla 38. Descripción Metadato MODE.9.1. – Nivel de Seguridad. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE. 9.1.1 – Nivel de Acceso

MODE 9.1.1. – NIVEL DE ACCESO			
Nombre oficial	MODE 9.1.– Nivel de Seguridad – Nivel de acceso		
Sub- elemento de	MODE 9.1 – Nivel de Seguridad		
Definición	"Término normalizado de acuerdo con un esquema de valores que indica el nivel de acceso de la entidad" (p.35).		
Aplicabilidad	Contexto de aplicación a todas las entidades.		
Obligación	Condicional – "Debe utilizarse si el documento o la regulación tiene un nivel de seguridad en su jurisdicción" (p.34).		
Automatizable	✓	**Repetible**	
Sub- Categorías	MODE 9.1.1. – Nivel de Acceso		
Valores	Esquema		Secreto Reservado Confidencial No clasificado
	Valor genérico		No aplica.
Compatibilidad	ISO 27001		Seguridad de información dentro de los modelos de aplicación (Uso)
Finalidad	✓ Determinar la categoría a la que se realiza la compatibilidad con el nivel de seguridad.		

Tabla 39. Descripción Metadato MODE.9.1.1. – Nivel de Acceso. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE. 9.2 – Permisos

MODE 9.2. – PERMISOS	
Nombre oficial	MODE 9.2.– Seguridad – Permisos

Sub- elemento de	MODE 9. –Seguridad		
Definición	“Autorización o acreditación de un agente o actividad, que determina sus derechos de acceso, uso y reutilización de los documentos.” (p.38).		
Aplicabilidad	Agente y actividad.		
Obligación	Condicional - “Debería utilizarse en organizaciones en las que las autorizaciones o acreditaciones de seguridad de los agentes regulan a qué documentos pueden acceder o mantener, o si el acceso a y el uso de documentos está restringido a actividades particulares” (p.38).		
Automatizable	✓	**Repetible**	✓
Sub- Categorías	No aplica.		
Valores	Esquema	No aplica.	
	Valor genérico	No aplica.	
Compatibilidad	ISO 27001	Seguridad de información dentro de los modelos de aplicación (Uso y categorización de los esquemas de seguridad establecidos en la norma)	
Finalidad	✓ Facilitar las autorizaciones correspondientes al uso y acceso que los documentos presentan en el sistema de seguridad, sin dejar de lado la reutilización de los mismos.		

Tabla 40. Descripción Metadato MODE.9.2. – Permisos. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE. 9.3 – Nivel de confidencialidad de la información

MODE 9.3. – Nivel de confidencialidad de la información	
Nombre oficial	MODE 9.3. – Seguridad – Nivel de confidencialidad de la información.
Sub- elemento de	MODE 9. –Seguridad
Definición	Categorización por parte de la organización acorde a niveles de seguridad en torno a un esquema de seguridad de información.
Aplicabilidad	Agente y actividad.

Obligación	Obligatorio – Aplicación de transferencia.		
Automatizable		**Repetible**	
Sub- Categorías	No aplica.		
Valores	Esquema	Bajo, medio, alto.	
	Valor genérico	No aplica.	
Compatibilidad	ISO 27001 –ISO 23081	Uso.	
Finalidad	✓ "Indicar el nivel de confidencialidad de la información contenida en el documento" (p.40).		

Tabla 41. Descripción Metadato MODE.9.3. – Nivel de confidencialidad. Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).

Descripción Metadato MODE. 9.4 – Sensibilidad de datos de carácter personal

MODE 9.4. – Sensibilidad de datos de carácter personal			
Nombre oficial	MODE 9.4. – Seguridad – Nivel de confidencialidad de la información.		
Sub- elemento de	MODE 9. –Seguridad		
Definición	Termino normalizado de acuerdo a la Ley estatutaria 1581 de 2012 reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por la cual se dictan disposiciones generales para la protección de datos personales.		
Aplicabilidad	Agente y actividad.		
Obligación	Condicional - Debe emplearse de acuerdo a lo estipulado por la normatividad atendiendo a todas las especificaciones.		
Automatizable		**Repetible**	
Sub- Categorías	No aplica.		
Valores	Esquema	Bajo, medio, alto.	
	Valor genérico	No aplica.	
Compatibilidad	ISO 23081	Uso.	
Finalidad	✓ Identificar el nivel de datos sensibles dentro de la información de la organización en función de determinar el nivel de sensibilidad de la organización.		

Tabla 42. Descripción Metadato MODE.9.4. – Sensibilidad de datos de carácter personal. . Fuente: elaboración propia. (2017), de acuerdo al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Versión 2.0 (Ministerio de Hacienda y Administraciones Públicas, 2016).