Cuaderno

8

Medidas de seguridad en los sistemas de gestión documental electrónica

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

UNIVERSIDAD DE LASALLE

CUADERNO

8

Seguridad en los sistemas de gestión documental electrónica

Johann Enrique Pírela Morillo

Directorio

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)

Francisco Javier Acuña Llamas
Comisionado Presidente

Oscar Mauricio Guerra Ford
Comisionado

Blanca Lilia Ibarra Cadena
Comisionada

María Patricia Kurczyn Villalobos
Comisionada

Rosendoevgueni Monterrey Chepov
Comisionado

Josefina Román Vergara
Comisionada

Joel Salas Suárez
Comisionado

Universidad de La Salle

Hno. Alberto Prada San Miguel
Rector

Adriana Patricia López
Decana
Facultad de Ciencias Económicas y Sociales

Nelson Javier Pulido Daza
Director
Programa de Sistemas de Información, Bibliotecología y Archivística

---

Edición a cargo de la Dirección General de Gestión de la Información y Estudios del INAI

1ª Edición, diciembre 2019

Impreso en México

Ejemplar de distribución gratuita

e-ISBN: 978-958-49-2268-7

CUADERNOS DE LA SERIE GESTIÓN DE DOCUMENTOS Y ADMINISTRACIÓN DE ARCHIVOS

CUADERNO

8

Seguridad en los sistemas de gestión documental electrónica

Johann Enrique Pírela Morillo

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

UNIVERSIDAD DE LA SALLE

Contenido

Presentación

La conservación de los documentos que generan las dependencias y en general cualquier sujeto obligado es un factor vital para la rendición de cuentas y la transparencia; circunstancia que se reglamentó con la entrada en vigor de la Ley General de Archivos (LGA), misma que cuenta con un respaldo constitucional expreso, la cual, entre otras bondades, contempla a los archivos históricos como fuentes de acceso público, lo que evitará que se clasifique como reservada o confidencial; la misma suerte tendrán aquellos archivos que tengan relación con violaciones graves a derechos humanos o delitos de lesa humanidad, por lo que la aplicación de la nueva norma tutelará también por la memoria histórica y la no repetición.

La norma reglamentaria cuenta con la integración de órganos colegiados para la debida tutela de la gestión documental (Sistema Nacional de Archivos), en la que formarán parte no solo el órgano garante nacional (INAI) y el Archivo General de la Nación, sino también la representación de cada instituto de transparencia local, para la toma de decisiones en materia archivística.

Cabe destacar la inclusión de archivos digitales en la LGA, con lo que se avanza hacia políticas más sustentables que ocuparán menores espacios físicos en cada sujeto obligado y de un gobierno sin papel (gobierno digital), aunado al hecho de la obligación del inicio de operaciones del Registro Nacional de Archivos, lo que permitirá un mejor manejo del caudal documental.

En este contexto el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), presenta los tomos 6 al 10 de la colección de cuadernos de la serie Gestión de Documentos y Administración de Archivos, los cuales abordarán temas preponderantes como los sistemas de gestión documental y administración de archivos; la gestión documental electrónica y su tratamiento; la Protección de datos personales y acceso a la información desde los archivos; la conservación documental y preservación digital; y los archivos y la planeación estratégica aplicada.

Los cuadernos de la serie Gestión de Documentos y Administración de Archivos constituyen una serie de guías técnicas metodológicas que orientan al conocimiento básico de los principales procesos documentales. Con ellos se ofrece un panorama general que no pretende agotar la muy diversa y compleja fenomenología de la actividad archivística, sino que busca poner en perspectiva los sistemas y métodos esenciales de la gestión de documentos y la administración de archivos.

La emisión de los cuadernos tiene además propósitos pedagógicos, ya que, por un lado, pueden constituirse como una herramienta auxiliar para apoyar las acciones de capacitación archivística que emprendan las instituciones gubernamentales, y por otro, buscan propiciar entre los no especialistas el reconocimiento de los sistemas, métodos e instrumentos de uso cotidiano en los archivos, cuya generación reclama con frecuencia la participación multidisciplinaria de otros profesionales en el seno de las instituciones gubernamentales.

Capítulo 1
Fundamentos conceptuales

Sumario:

Capítulo 1: Fundamentos conceptuales

1.1 Conceptos sobre seguridad en los sistemas de gestión documental electrónica

Un Sistema de Gestión de Seguridad de la Información (SGSI), según la Norma UNE-ISO/IEC 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Esto significa que se va a dejar de operar de una manera intuitiva y se tomará el control sobre lo que sucede en los sistemas de información y sobre los datos que maneja la organización. Esto nos permitirá conocer mejor nuestra organización, cómo funciona y qué podemos hacer para que la situación mejore.

La norma especifica que, como cualquier otro sistema de gestión, el SGSI incluye tanto la organización como las políticas, la planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. Es decir, tanto la documentación de soporte como las tareas que se realizan. Los sistemas de gestión que definen las normas ISO siempre están documentados, ya que, por un lado, es la mejor manera de formalizar normas e instrucciones y, por otro, son más fáciles de transmitir y comunicar, lo cual no sucedería si se confía en un traspaso de información verbal informal.

Esta norma es compatible con el resto de las normas ISO para sistemas de gestión (UNE-EN ISO 9001 y UNE-EN ISO 14001) y todas poseen idéntica estructura y requisitos comunes, por lo que se recomienda integrar el SGSI con el resto de los sistemas de gestión que existan en la empresa para no duplicar esfuerzos.

El objetivo del sistema de gestión proyectado es aumentar la seguridad de la información mediante el sostenimiento de la integridad, disponibilidad y confidencialidad de la información, manejada en los sistemas de información donde esta es depositada y gestionada.

Incluso cuando no exista un sistema de gestión formal, el amplio conocimiento actual de estos sistemas ayuda a que las principales características de la norma sean comprensibles para la mayoría de la gente, y que para explicarla en detalle sea suficiente con incidir en las diferencias fundamentales, a saber, que con un SGSI lo que tratamos es de gestionar la seguridad de la información de nuestra organización.

Al hacer una aplicación conceptual de los atributos que se deben mantener en seguridad para que los Sistemas de Gestión Documental Electrónica puedan cumplir con su cometido, como se comentó, Mena (2008, p. 26) hace una propuesta de requerimientos funcionales para la gestión de documentos electrónicos, y señalan que es posible lograrlo desde el Modelo de Cadena de Preservación (MPC) producido por InterPares2; para ello, se basa en este modelo puesto que se cimienta idealmente en el concepto del ciclo de vida de los documentos y el modelo de custodia continua de los mismos.

En este sentido, la estructura de los requerimientos funcionales de la elaboración de documentos electrónicos debería contener como mínimo los siguientes elementos:

- ✓ Formas de los documentos
- ✓ Archivo y registro
- ✓ Esquemas de metadatos
- ✓ Privilegios de archivos para la elaboración de documentos archivísticos

En cuanto al diseño de sistemas de identificación, valoración y mantenimiento, este se basa en tareas tales como:

- ✓ Cuadros de clasificación
- ✓ Registro de entrada y salida
- ✓ Esquema de metadatos para la identificación, valoración y mantenimiento de los documentos archivísticos
- ✓ Calendario de conservación
- ✓ Recuperación del sistema de identificación, valoración y mantenimiento de los documentos archivísticos
- ✓ Procedimientos para mantener la autenticidad de los documentos archivísticos
- ✓ Privilegios de acceso para el sistema de identificación, valoración y mantenimiento de los documentos

Ahora bien, MoReq2 identifica una serie de requisitos funcionales para la gestión de documentos electrónicos de archivo mediante un sistema de gestión de documentos de archivo (SGDEA), y aunque los expone de forma muy detallada, también permite ver de forma más general una serie de condiciones implícitas en el documento electrónico y cómo se interrelaciona con uno tradicional, relación que en la norma es denominada híbrida o con requisitos mixtos. La norma plantea estos requisitos desde los siguientes supuestos:

Gestión de documentos de archivo no electrónicos

- ✓ El SGDEA debe reflejar y gestionar del mismo modo, los documentos tradicionales y los electrónicos.
- ✓ Debe definir un cuadro de clasificación que lógicamente contenga los dos modelos de documentos y permita la gestión integrada de ambos.
- ✓ Los documentos mixtos deberán utilizar el mismo título y código de referencia numérica, con una especificación añadida que indique que se trata de un expediente mixto.
- ✓ Debe contener una serie de metadatos atendiendo a la especificidad de expedientes físicos o tradicionales y sus elementos complementarios lógicos.
- ✓ Se debe garantizar la recuperación del expediente mixto de acuerdo con los metadatos de los documentos electrónicos de archivo y en papel asociados a él.
- ✓ Deben tener los mismos niveles de seguridad los documentos electrónicos que los documentos físicos (en cuanto a privilegios se refiere).

Conservación, eliminación o transferencia de expedientes mixtos

- ✓ Se debe permitir la asignación y aplicación de normas de conservación a los expedientes mixtos.
- ✓ Deben estar asociados a los documentos tradicionales para en un momento determinado identificar la existencia y la ubicación de los documentos de archivo electrónicos o mixtos incluidos los metadatos.
- ✓ Requiere que exista la trazabilidad en entrada, salida y préstamo de expedientes; de igual forma, consignar estos datos para el eventual momento en que se tenga que especificar quién tiene el documento o expediente.

Flujos de tareas

- ✓ Debe estar establecida una serie de pasos que conforman en su totalidad un flujo de tareas, tales como traslados, préstamos o consultas.
- ✓ No se debe limitar el número de tareas o pasos.
- ✓ No se debe permitir que los usuarios modifiquen los flujos, las tareas o actividades de los documentos.
- ✓ Se debe gestionar, pero el administrador podrá observar la trazabilidad del documento.

Firmas electrónicas

- ✓ Se requieren únicamente si existe la necesidad de gestionar documentos con firmas electrónicas.
- ✓ Estas se deben visualizar en diferentes herramientas tecnológicas.
- ✓ Deben mantener metadatos relacionados con el proceso de verificación de la firma electrónica.

Encriptación:

- ✓ Proceso que se utiliza para codificar un documento electrónico con el fin de impedir el libre acceso a este; esto garantiza la seguridad de cierto tipo de información.
- ✓ Cuando se gestione un documento encriptado deberá conservar los metadatos al momento de ser remitido y recibido.

Filigranas electrónicas y elementos similares

- ✓ Debe marcarse, si se requiere, con la información del propietario o su procedencia.
- ✓ Sobre la imagen de bits se superpone un patrón complejo que hace visible lo invisible, que solo se puede eliminar recurriendo a un algoritmo y a una clave de seguridad.

Metadatos

- ✓ Deben ser inmodificables.
- ✓ Deben ser descriptivos de seguridad, identificadores.

Debido a que el mismo documento hoy en día puede desenvolverse en una diversidad de sistemas, el Archivo General de la Nación (2017) sugiere que la gestión debe configurar ciertos requisitos mínimos, dentro de los cuales debe estar sustentado por políticas y procedimientos claros; dicho Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) debe permitir como mínimo:

- ✓ Integridad archivística de los fondos, a partir de agrupaciones documentales (expedientes, series, subseries), manteniendo el vínculo archivístico de los documentos.
- ✓ Armonizar la gestión documental en ambiente físico y electrónico.
- ✓ Atender a los principios archivísticos: procedencia, orden original, integridad de los fondos y descripción archivística.
- ✓ Contemplar la administración de los instrumentos archivísticos.
- ✓ Considerar los procesos de transferencia en aplicación de las TRD.

- ✓ Asegurar la conservación de los documentos electrónicos de archivo a largo plazo.
- ✓ Utilización de estándares de interoperabilidad para el intercambio de información entre diferentes sistemas de información internos y externos (AGN, 2017).

En esa misma medida el SGDEA debe tener en cuenta los siguientes elementos:

Ilustración 1. Elementos complementarios del SGDEA

Fuente: Archivo General de la Nación, 2017.

Así las cosas, la integración del documento electrónico se configura y articula de diversas maneras con los sistemas y con los principios archivísticos. Acorde a ello sugiere el AGN con respecto al SGDEA que:

La producción y procesamiento de documentos electrónicos mediante diferentes sistemas de información, requiere de la generación de políticas de gestión documental y la adopción de estándares técnicos internacionales, así como de un modelo conceptual y operativo de lineamientos para la administración organizacional tendentes a la aplicación de tecnologías de la información y la comunicación (TIC) en procesos de gestión documental, orientados a garantizar la autenticidad, integridad, disponibilidad, y preservación a largo plazo de los documentos de archivo (AGN, 2017).

El número de requisitos funcionales estipulados en las normas es elevado. A modo de ejemplo, se sistematizan los 275 requisitos que aparecen en el modelo ISO 16175-2 para la GSDE, tal y como se agrupan en la tabla siguiente:

Tabla 6. Cómputo de requisitos funcionales propuestos para el SGDE

CREACIÓN (87)	MANTENIMIENTO (110)	DIFUSIÓN (50)	ADMINISTRA-DOR (33)
1-Captura (9) 2-Metadatos (11) 3-Agrupaciones documentales (5) 4-Apoyo a la importación masiva, exportación y la interoperabilidad: formatos, documentos compuestos, correo electrónico (12) 5-Identificación del documento (7) 6-Clasificación (13) 7-Cuadro de clasificación: establecimiento de cuadros, niveles, clasificación de los procesos (30)	1-Metadatos y procesos de gestión de documentos auténticos y fiables y trazabilidad de movimientos de documentos (16) 2-Controles de acceso y seguridad, controles de acceso, establecimiento de controles de seguridad, asignación de niveles, cumplimiento de controles, categorías de seguridad (30) 3-Autenticación, cifrado y medidas tecnológicas de protección. 4-Gestión de documentos híbridos: expedientes y documentos (10) 5-Retención y disposición: CC, establecimiento, aplicación, ejecución, migración, exportación, destrucción, actuación ante no electrónicos; documentación de acciones de disposición, revisión de la disposición (55)	1-Búsqueda, recuperación (27) y 2-Representación, visualización de los documentos, impresión, documentos editados (23)	1-Funciones del administrador 2-Administración de metadatos, 3-informes 4-Copia de seguridad y recuperación 5-Definición de niveles: usuario/ usuario autorizado/ Administrador de documentos (archivero)/ Administrador del sistema de GD

Fuente: Elaboración propia, basada en ISO 16175-2.

1.2 Estándares y protocolos de seguridad

Para el desarrollo del contenido de esta política, se han tenido en cuenta las siguientes normas y buenas prácticas: Actualizar listado de normas con las correspondientes utilizadas en la entidad en cuestión. - ISO 15489. Información y documentación. Gestión documental.

- ✓ UNE-ISO/TR 18492 IN: Conservación a largo plazo de la información basada en documentos.
- ✓ UNE-ISO 30300. Información y documentación. Sistemas de gestión para los documentos.
- ✓ UNE-ISO 23081. Información y documentación. Procesos de gestión de documentos. Metadatos para la gestión de documentos.
- ✓ UNE-ISO7TR 26122 IN: Información y documentación. Análisis del proceso de trabajo para la gestión de documentos.
- ✓ UNE 139803:2012. Requisitos de Accesibilidad para contenidos en la web.

Es responsabilidad del área de información en lo concerniente a la elaboración, modificación, distribución y control de un Manual del Sistema de Gestión de Seguridad de la Información.

Este documento será revisado como mínimo una vez al año para efectos de actualización, o por cualquier otro motivo que muestre resultados diferentes a los planeados por el Sistema de Gestión de Seguridad de la Información de la empresa.

1.3 Modelo de requisitos para la seguridad de los sistemas de gestión de documentos electrónicos

Si bien el modelo PDCA, del inglés *Plan-Do-Check-Act*, en español, Planificar-Hacer-Verificar-Actuar) conocido también como "Ciclo o Rueda de Deming", es el estándar formal de ISO, este se construye sobre una base que no necesariamente se aplica a todas las organizaciones, sobre todo cuando estas no se han involucrado en procesos relacionados con normas ISO, por ello, con una base práctica se presenta el siguiente modelo, el cual no omite ni restringe las actividades señaladas en el esquema formal, sino que se vale de ellas para sustentar un formato práctico de actividades que deben ser abarcadas para lograr un adecuado nivel de seguridad de la información en las áreas de TIC en cualquier tipo de organización.

Este modelo puede ser perfeccionado y modificado en el futuro dado que su estructura se debe ajustar a los constantes cambios que surgen en las organizaciones como sistema dinámico.

La particularidad del modelo que se presenta a continuación reside en su aspecto operativo y práctico, puesto que se considera su estructuración, formación e implementación bajo cuatro etapas.

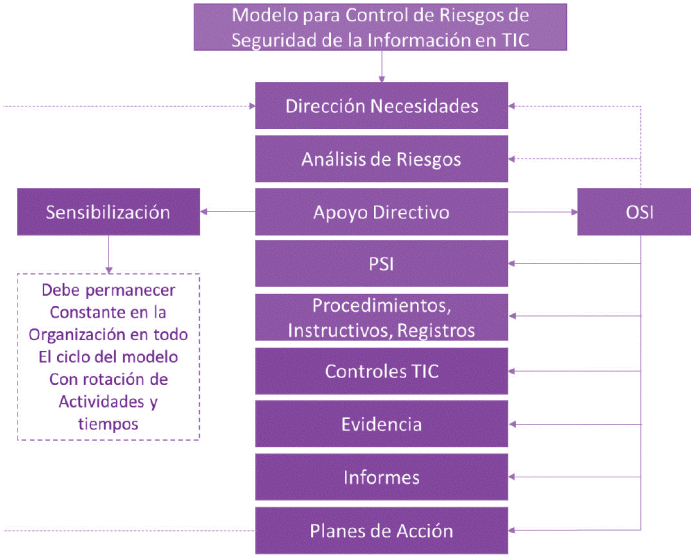
1. Documentación del sistema;
2. Implementación del sistema;
3. Evaluación del sistema a través de auditorías internas y externas, y
4. Mejoramiento continuo de la eficacia del sistema mediante el análisis de datos.

Estas fases contemplan el conjunto de actividades que de ellas se desprenden y están ligadas mediante la secuencia de actividades que es necesario desarrollar a fin de elaborar y aplicar correctamente el modelo.

Este modelo considera los principales elementos incluidos en las diversas normas y estándares internacionales relacionados con la seguridad de la información, por lo que creemos que apoya la concreción de un gobierno con una política de TIC, lo que a su vez abarca un aspecto mayor al diseño inicial, ya que esto implica que no solo cubre temas de seguridad y de riesgos, sino que al mismo tiempo apoya a lograr aspectos de estructura organizacional, descripciones de cargo y tareas, definiciones de misión y visión, no solo en el ámbito gerencial, sino en cada área.

La Figura 1 presenta el modelo en forma esquemática. Este esquema resume y agrupa todas las actividades y se debe entender que muchas de ellas llevarán un ciclo continuo de mejora.

Figura 1.



Las actividades son secuenciales y a la vez se comportan en un estado cíclico con periodos de tiempo en su ciclo, que varían dependiendo de cada organización y del estado de avance que esta última tenga respecto a temas de seguridad de la información.

A continuación, se presenta una descripción de cada una de las fases y actividades que cada una de las organizaciones consideran:

Dirección Necesidades: Corresponde al levantamiento de todas las actividades relacionadas con los impactos que la organización pueda tener en relación con la seguridad de la información.

Análisis de Riesgos: Corresponde a evaluar todos los potenciales riesgos en los cuales se pueda ver envuelta la organización por aspectos emanados de las TIC y que impactan en la seguridad de la información.

Apoyo directivo: Corresponde a la presentación del resultado del diagnóstico y el análisis de cada uno de los riesgos con el fin de conseguir el apoyo para concretar la implementación de la seguridad de la información (presupuestos, personal, capacitación, etc.) Durante los procesos de capacitación que se realizan con los colaboradores de la entidad se hace referencia a dichos principios de seguridad de la información contenidos en la norma ISO / IEC27001 y la forma de adaptarlos.

Oficial de Seguridad de la Información (OSI): La organización debe designar a un archivista profesional que apoye, dirija y pueda llevar el control de implementación, ejecución y posterior seguimiento del modelo de seguridad de la información.

Políticas de Seguridad de la Información (PSI): Corresponde al diseño de las Políticas de Seguridad de la Información de la organización, que se encuentran definidas en la Política del Sistema de Gestión de Seguridad de la Información y corresponde al cumplimiento de la normatividad legal vigente, con el objeto de gestionar y administrar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la entidad u organización.

Elaboración de procedimientos, instructivos y registros: Corresponde al desarrollo de documentos que formalizan el cómo se deben realizar las actividades y qué información es la que se debe retener como evidencia para dar conformidad a las PSI.

Controles TIC: En esta etapa se diseñan y definen los procesos, objetivos de control, controles y evidencias formales de las actividades de seguridad que darán sustento a los procesos de revisión o auditorías del modelo.

Evaluación y auditoría: En esta etapa se debe revisar que todos los procesos de TIC se están cumpliendo y llevando a cabo adecuadamente, lo cual será evaluado por el mismo proceso de auditoría (interna y/o externa).

Evidencia: En esta etapa se busca verificar de manera adecuada que los registros de TIC para todos sus procesos y controles estén disponibles para cualquier tipo de revisión, particularmente los procesos de auditoría.

Informes: Esta etapa contempla la confección de dictamen, datos o referencias del proceso de revisión que derivarán en actividades de mejora al modelo y con revisiones por parte de la dirección de la organización que permitan confeccionar adecuados planes de acción.

Planes de acción: Esta etapa consiste en poner en práctica lo programado conforme a los plazos y actividades que fueron indicados en el proceso de auditoría. Estos planes pueden conformar la revisión y ajustes de todo tipo de actividades ya sea a nivel de procesos de seguridad, de evidencias, de políticas o de cualquier otra actividad que sea identificada.

Sensibilización: Esta etapa (incluida en ambas fases del modelo) permite alertar a la organización sobre la importancia de mantener la seguridad de la información.

Capítulo 2
Cumplimiento de medidas de seguridad

Sumario

Capítulo 2
Cumplimiento de medidas de seguridad

2. Cumplimiento de medidas de seguridad

2.1. Validación del cumplimiento de medidas de seguridad

Para hacer la validación del cumplimiento de medidas de seguridad, recomendamos tomar un estándar como marco de referencia, que puede ser la metodología MAGERIT – Versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, desarrollada por el Consejo Superior de Administración Electrónica del gobierno de España. Esta metodología brinda una aproximación metódica con herramientas que no apoyan la improvisación. A lo largo del desarrollo de la metodología permite establecerse en paralelo con la metodología de medición de riesgo operativo de cualquier organización para así poder comparar los peligros o incidentes de seguridad de la información con los demás riesgos operativos.

Criterios de evaluación de riesgos

- ✓ Las identificaciones de los riesgos asociados a los procesos se deben realizar conjuntamente con los funcionarios involucrados en cada uno, el control y seguimiento se ejecutará de una manera cíclica para así

mantener actualizados los factores de riesgo y poder medir su impacto de manera oportuna.

- ✓ El reconocimiento y reporte de los factores y eventos de riesgo es responsabilidad de cada área.
- ✓ Los responsables de cada área se encargarán de validar, documentar y firmar el registro de eventos o incidentes de seguridad de la información, para luego presentar un informe a quien coordine la operación.
- ✓ Los niveles de riesgo aceptables se muestran en la siguiente tabla, con su respectivo nivel de aceptación:

Nivel de Riesgo	Riesgo de Seguridad de Información - RSI	Tratamiento del RSI
Bajo	Despreciable	Los riesgos ubicados en este nivel se consideran "insignificantes", los cuales se administrarán con procesos rutinarios controlando que no suban a otro nivel de la escala.
	Bajo	
Moderado	Medio	Los riesgos ubicados en este nivel se consideran "aceptables", la responsabilidad de mejorar y monitorear los controles será de los encargados de los procesos. Estos riesgos pueden ser objeto de estudio para su tratamiento.
Alto	Alto	
Extremo	Muy alto	Los riesgos ubicados en este nivel se consideran "no aceptables", el tratamiento a estos riesgos debe ser inmediato, implementando planes de acción expeditos para que el nivel de riesgo baje, teniendo en cuenta las prioridades de cada organización.
	Critico	

Es preciso destacar que no todos los riesgos son susceptibles de ser tratados de manera inmediata. Esta decisión depende del nivel en que se encuentre dentro de la matriz o perfil de riesgo. Los riesgos de nivel muy alto y crítico son considerados como inaceptables y se les dará prioridad de acción.

Opciones de tratamiento de riesgos

El tratamiento que se decida darle a cada riesgo debe estar alineado con los objetivos de la organización. Este tratamiento implica su preparación e implementación por parte de los responsables de los procesos, dependiendo de la opción que se elija :

- ✓ Evitar Riesgo: Decidir no proceder con la actividad que probablemente genera el riesgo (si es pertinente).
- ✓ Control del Riesgo: Poner en práctica controles que reduzcan la probabilidad de ocurrencia y la posible consecuencia.
- ✓ Transferencia del Riesgo: Compartir el riesgo o buscar apoyo con terceros (subcontratación, otras áreas, pólizas de seguro, etc.).
- ✓ Aceptación del Riesgo: Tolerar el riesgo, sin poner en marcha planes de acción.

Plan de tratamiento de riesgos

Después de efectuar los análisis de riesgos, el comité de seguridad de la información junto con cada una de las áreas involucradas, debe efectuar un plan de tratamiento de riesgos, para aquellos considerados como críticos en los activos bajo su responsabilidad.

Declaración de aplicabilidad

La declaración de aplicabilidad proporciona un resumen de las decisiones concernientes al tratamiento de los riesgos. La justificación de las exclusiones permite validar que ningún control se omita involuntariamente, por ello la declaración de aplicabilidad del Sistema de Gestión de Seguridad de la Información se encuentra registrada en el documento "Declaración de aplicabilidad".

Requisitos de Documentación

Los parámetros concernientes a la gestión documental de cualquier organización deben estar alineados y definidos en el documento: "Manual de Gestión Documental", en el que se definen las acciones de gestión necesarias para:

a) Revisar y actualizar los documentos según sea necesario.
b) Verificar que los cambios y el estado de actualización de los documentos estén identificados.
c) Comprobar que las versiones más recientes de los documentos están disponibles en físico y electrónico.
d) Confirmar que los documentos permanezcan legibles y fácilmente identificables.
e) Cerciorarse que los documentos estén disponibles para quienes los necesiten, y que se apliquen los procedimientos pertinentes, de acuerdo con su clasificación, para su almacenamiento, transferencia y disposición final dentro del ciclo de vida de los documentos.
f) Vigilar que los documentos de origen externo estén identificados.
g) Asegurar el control en la distribución de documentos.
h) Impedir el uso de documentos obsoletos.

Detección y respuesta a los incidentes de seguridad

Desde el inicio del proceso debe establecerse y mantenerse una metodología de gestión de incidentes de seguridad de la información, ya que allí se define la responsabilidad y autoridad con respecto a su manejo e investigación.

Seguimiento y revisión del sistema SGSI

En la metodología de gestión de incidentes de seguridad de la información, debe establecerse la responsabilidad y autoridad con respecto al manejo e investigación de incidentes de seguridad de la información.

Auditorías internas del SGSI

Con esta metodología se define la responsabilidad y autoridad en las auditorías de seguridad de la información.

Indicadores del Sistema de Gestión de Seguridad de la Información

A continuación se definen los indicadores para medir los objetivos del Sistema de Gestión de Seguridad de la Información:

Gestión de riesgos de seguridad

Número de revisiones efectuadas por la alta dirección para cada año
Porcentaje de ejecución de los planes de tratamiento de riesgos
Porcentaje de procesos cuyos activos de información han sido identificados y clasificados

Porcentaje de procesos cuyos activos de información / datos privados tienen un análisis documentado de riesgos
Porcentaje de activos de información del proceso que han sido sujetos a un análisis de riesgos documentado
Porcentaje de procesos cuyos datos privados han sido identificados y clasificados
Porcentaje de procesos cuyos activos de información / datos privados tiene un plan de mitigación documentado
Porcentaje de activos de información del proceso que tiene un plan de mitigación documentado

Gestión segura del riesgo humano

Porcentaje de cargos que incluyen la seguridad de la información en las responsabilidades, habilidades
Porcentaje de usuarios por área que han contemplado el registro de antecedentes antes de tener acceso a la información
Porcentaje de cargos que incluyen la seguridad de la información en las evaluaciones de desempeño
Porcentaje de usuarios que contemplaron el plan de educación, conciencia y entrenamiento en seguridad en el último año

Seguridad de aplicaciones con acceso

Porcentaje de aplicaciones acreditadas
Porcentaje de aplicaciones que cuyo acceso se controla basado en roles

Porcentaje de aplicaciones evaluadas en el último año
Porcentaje de aplicaciones cuyos usuarios y privilegios han sido certificados en el último año por los directivos

Continuidad

Porcentaje de procesos cubiertos por un análisis de impacto al negocio
Porcentaje de procesos que tienen definidas las actividades de continuidad

Revisión del SGSI por la dirección

La alta dirección en cada organización, revisará, en coordinación con el Comité de Seguridad de Información, la efectividad de la implementación del Sistema de Gestión de Seguridad de la Información y el comportamiento de medición de sus indicadores cada vez que se estime conveniente; para ello, podrá definirse un plan de reuniones periódicas, que en ningún caso deberá ser inferior a una vez al año. Los temas que deberán tratarse en el comité serán:

Aspectos	Registro
Revisión de la política y objetivos del sistema de gestión	Acta
Resultados del análisis de riesgos y seguimiento a los planes de tratamiento establecidos	Seguimiento plan de tratamiento de riesgos
Evaluación de conformidad con los requisitos legales aplicables	Acta

Estado de investigación y análisis de incidentes de seguridad de la información	Acta
Resultados de auditorías internas	Informe de auditorías internas
Acciones correctivas y preventivas	Acta
Cambios al Sistema de Gestión de Seguridad de la Información	Acta
Recomendaciones para la de mejora	Acta
Seguimiento de revisiones previas	Acta
Desempeño financiero y costos relacionados con la seguridad de la información	Acta
Necesidad de recursos	Acta

Resultados de la revisión

De conformidad con el contenido del Sistema de Gestión de Seguridad de la Información, así como los procesos, la Alta Dirección en cada organización, toma las acciones necesarias con el propósito de mejorar su eficacia y el control de los riesgos de seguridad de la información.

El Comité de Seguridad de la Información se reúne y revisa la información del sistema de gestión, elaborando los ajustes

necesarios, teniendo como referencia la política del sistema. Allí se determinan las directrices, se solicitan los recursos, se erigen los planes de tratamiento de riesgos a la alta gerencia. De cada revisión de la dirección se deja constancia en un acta de reunión describiendo el análisis realizado por el equipo ejecutivo y las decisiones tomadas con respecto a la eficacia y mejora del sistema de gestión y la necesidad de recursos.

Mejora del SGSI

Todas las áreas, según la información recolectada, se encargan de elaborar planes de mejoramiento continuo de acuerdo con las Políticas y Objetivos de Seguridad de la Información, apoyado por la alta dirección y el Comité de Seguridad de la Información que participan activamente en el desarrollo y evaluación de estos planes.

Se deben revisar y monitorear los siguientes elementos que componen el SGSI:

- ✓ Contenido de los procedimientos: Creación, modificación y actualización de los procedimientos tanto en estructura como en contenido, buscando la descripción real de cada una de las actividades que se desarrollan dentro de la organización. Lo anterior incluye: descripciones, caracterización, controles, objetivos, formatos, etc.
- ✓ Actualización de la intranet: Modificación del contenido de la intranet según las modificaciones de los procesos y la creación de los mismos.
- ✓ Manual SGSI: Actualización o modificación del manual por las siguientes razones:

- Cambios o ajustes en el marco normativo aplicable a la organización.
- Cambios en la metodología (riesgos, controles fuentes de información, etc.).
- Inclusión de nuevas estrategias.
- Cambios por determinación de los entes de control.
- Cambios por estructura organizacional.

Perfeccionamiento del riesgo en el tiempo, es decir, si con la aplicación de controles ha ido disminuyendo.

Conjunto de descripciones detalladas de los incidentes, por proceso, funcionario y área.

Acciones preventivas y correctivas

Este procedimiento aplica a todo el Sistema de Gestión de Seguridad de la Información y se inicia con la identificación de la no conformidad hasta que es eliminada o hasta que es controlada.

Definiciones

Acción correctiva: acción implementada para lograr la eliminación de una no conformidad detectada.

Acción preventiva: acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencial indeseable.

Corrección: acción tomada para eliminar la no conformidad.

No conformidad: incumplimiento de un requisito del SGSI.

Identificación de las no conformidades reales y potenciales

La alta dirección debe buscar el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información, detectando las no conformidades reales o potenciales que pudieran afectar su operación.

Los problemas existentes "no conformidades reales" pueden ser detectados por cualquiera de las siguientes formas:

- ✓ Registro de incidentes.
- ✓ Observaciones en las auditorías de seguridad de la información.
- ✓ Bajos índices de gestión en cualquiera de las áreas de la organización.
- ✓ Observaciones hechas por los mismos colaboradores de la organización.

Los problemas que pueden convertirse en no conformidades "no conformidades potenciales" pueden ser encontrados en cualquiera de las siguientes actividades:

- ✓ Comentarios de los ciudadanos y de los funcionarios.
- ✓ Observaciones de los ciudadanos en las encuestas de satisfacción que se realicen.
- ✓ Observaciones realizadas por medio de las auditorías de seguridad de la información.
- ✓ Tendencias en los índices de gestión de las áreas.
- ✓ Observaciones realizadas por los mismos funcionarios o servidores de la organización.

Corrección de las no conformidades

Una vez que se hace la plena identificación de la no conformidad existente, el tratamiento definido por la organización incluye:

- ✓ Análisis de causas mediante los métodos estadísticos o inductivo-deductivos que se consideren apropiados.
- ✓ Elaboración del plan de acción, en donde se definen:

  - Actividades que se emprenderán para la eliminación de la no conformidad.
  - Responsables de las actividades definidas para la eliminación de la no conformidad.
  - Plazos para la puesta en marcha y revisión de los resultados obtenidos con el plan de acción.
  - Evaluación de la efectividad de las acciones emprendidas para eliminar la no conformidad.

Prevención de las no conformidades

Cuando se detecta una situación que pudiera ser causante de no conformidades dentro del SGSI, la organización, dependiendo de la actividad en donde se detectó la situación y los posibles problemas que conllevaría su aparición (auditorías, grupos de trabajo, etc.), tomará medidas concretas para atender esas no conformidades potenciales según su complejidad, en donde se incluyen responsables, plazos, tareas por cumplir y próximas revisiones con el responsable.

Registro de las no conformidades reales y potenciales

El registro de las no conformidades reales y potenciales debe ser elaborado por el responsable del proceso o área en el documento "Formato de Acciones Preventivas y Correctivas". Este formato servirá como soporte para el seguimiento del tratamiento de la no conformidad real o potencial.

Resultados de las acciones correctivas y preventivas

El responsable del proceso, luego de detectar la no conformidad real o potencial y de planear las medidas correctivas o preventivas a que haya lugar, asentará en el formato de registro "Seguimiento resultado acción preventiva y correctiva", los resultados que se obtuvieron con tales acciones evidenciando la efectividad de las mismas.

Elementos y capacidades para lograr la implementación del Sistema de Gestión de Documentos Electrónicos de Archivo

Con la claridad de las directrices que hemos venido comentando a lo largo del documento, algunas de carácter institucional y otras suprainstitucionales, se deben desarrollar y fortalecer varias capacidades en la entidad y su personal para lograr la implementación del Sistema de Gestión de Documentos Electrónicos de Archivo. A continuación, resaltamos las principales capacidades:

Capacidades	Descripción
Captura e ingreso de documentos	1. Los documentos electrónicos generados o recibidos en procesos de gestión y administración de las entidades proceden de fuentes internas y externas. 2. Los documentos electrónicos pueden presentar distintos formatos y su autoría puede ser muy diversa. Además, se pueden recibir como documentos simples o como expedientes compuestos por varios documentos. 3. Los documentos electrónicos pueden recibirse a través de distintos canales de comunicación, como redes de área local, redes de área extensa, correo electrónico, fax y correo postal (que se escaneará) y presentar frecuencias de llegada y volumen variables. Nota: Para respetar toda esa diversidad, es preciso un sistema flexible y dinámico de entrada, que permita controlar adecuadamente la captura de documentos. (Moreq - Programa IDA comisión europea, 2001).
Cuadros de clasificación y organización documental de los expedientes	El cuadro de clasificación constituye el elemento clave de cualquier SGDEA, este define el modo en que los documentos electrónicos de archivo se organizarán en expedientes, en cuadros de clasificación, así como las relaciones entre dichos expedientes. (Moreq - Programa IDA comisión europea, 2001).

Capacidades	Descripción
Gestión de metadatos	La Información estructurada o semiestructurada permite la creación, la gestión y la utilización de documentos de archivo a lo largo del tiempo, tanto dentro de los ámbitos en que se crearon como entre ellos. Cada tipo de organización y de aplicación presenta unas necesidades y tradiciones propias que pueden variar enormemente. Así, ciertas entidades precisarán una indexación basada en las denominaciones de las cuentas y las fechas de transacción, mientras que otras recurrirán a una estricta jerarquía numérica; algunas entidades deberán definir volúmenes en función de los ejercicios presupuestarios, mientras que en otras será más importante centrarse en los controles de acceso, ya sea por razones de seguridad o por motivos relacionados con la propiedad intelectual, etc. Por consiguiente, esta capacidad se limita a sugerir unos requisitos mínimos de carácter genérico que luego se podrán personalizar. Entre ellos se incluye una lista de ciertos elementos de metadatos que el SGDEA ha de poder capturar y procesar. (Moreq - Programa IDA comisión europea, 2001).
Gestión de flujos de trabajo	Los requisitos enumerados en esta sección solamente resultan pertinentes cuando el SGDEA incluye algún recurso relacionado con el flujo de tareas. Estos van desde las funciones de rutina hasta los instrumentos de flujo de tareas más sofisticados, que se pueden conseguir vinculando al SGDEA un producto de flujo de tareas (BPM) creado por terceros. Las tecnologías de flujo de tareas transfieren objetos electrónicos entre los participantes, sometiendo todo el proceso al control automático de un programa. En el contexto de los SGDEA, el flujo de tareas se utiliza para trasladar documentos electrónicos de archivo entre usuarios y departamentos. Por lo general se recurre a él en: • La gestión de procesos o tareas vitales, como los procedimientos de registro y procedimientos de selección de expedientes o documentos de archivo.

Capacidades	Descripción
	• La verificación y aprobación de los documentos de archivo antes de proceder a su registro. • La subdivisión de documentos de archivo o expedientes, de forma controlada, de usuario a usuario, con vistas a la realización de determinadas acciones, tales como la comprobación de un documento o la aprobación de una nueva versión. • La comunicación a los usuarios de la disponibilidad de documentos de archivo. • La distribución de documentos de archivo. • La publicación de documentos de archivo en la Red (Word Wide Web). La capacidad de los sistemas de flujos de tareas va desde la simple subdivisión (derivación, como la verificación y aprobación de un documento antes de grabarlo) al manejo de un volumen elevado de transacciones, en las que pueden presentarse circunstancias excepcionales, y a la presentación de informes sobre el rendimiento individual y del sistema. (Moreq - Programa IDA comisión europea, 2001).
Gestión de flujos electrónicos	Estos requerimientos de flujos electrónicos contienen las mismas características del anterior pero donde solo son documentos electrónicos.
Presentación, recuperación y búsqueda	1. Una parte esencial del SGDEA es la capacidad para que el usuario recupere expedientes y documentos de archivo. Esta opción abarca la búsqueda cuando se desconocen detalles concretos y su presentación. 2. La presentación consiste en crear una representación en pantalla (“visualización en pantalla”) o en su impresión, o bien en su reproducción en video o en audio. 3. El acceso a expedientes y documentos de archivo y su posterior visualización exigen una gama amplia y flexible de funciones de búsqueda, recuperación y presentación que respondan a las necesidades de los distintos tipos de usuarios. (Moreq - Programa IDA Comisión Europea, 2001).

Capacidades	Descripción
Retención y disposición	1. En esta capacidad se trabaja un aspecto fundamental de la gestión de documentos de archivo que viene dado por el uso de normas de conservación que rigen la eliminación de los documentos de archivo de los sistemas activos o en funcionamiento. 2. Las normas de conservación determinan el tiempo que el SGDEA debe conservar los documentos de archivo y su destino. Trata los temas de retención y disposición final de documentos (Moreq - Programa IDA comisión europea, 2001).
Seguridad y controles	Las organizaciones han de ser capaces de controlar a quién se permite el acceso a los documentos de archivo y en qué circunstancias, pues estos pueden contener información reservada de carácter personal, comercial u operativo. También puede ser conveniente restringir el acceso a los usuarios externos. Por ejemplo, en ciertos países donde la legislación sobre la libertad de información da acceso a determinados documentos de archivo públicos, los ciudadanos pueden desear consultar los documentos, además se enumeran pistas de auditoría, controles de autenticidad, autenticación, control de información, entre otros. (Moreq - Programa IDA comisión europea, 2001). La seguridad de los documentos de archivo abarca también la capacidad de protegerlos ante cualquier fallo del sistema mediante la creación de copias de seguridad y la posibilidad de restaurar los documentos de archivo a partir de estas.
Requerimientos no funcionales	En la práctica, los requisitos no funcionales son primordiales para el éxito de estos sistemas. Si bien los requisitos no funcionales suelen ser difíciles de definir y cuantificar con objetividad, es importante identificarlos, al menos en términos generales, para que puedan estudiarse. Así, algunos de esos requisitos son comunes a numerosas clases de sistemas de TIC. Esta capacidad intenta ofrecer una lista de cuestiones que los usuarios deberán tener en cuenta a la hora de establecer sus requisitos.

Se evidencia que estos habilitadores o componentes de la organización, como de TIC se basan en estándares internacionales como la ISO 15081, ISO 30300 y Moreq, por lo tanto, se encuentran suficientemente sustentados y soportados, indicando que corresponden a habilitadores claves para la implementación del SGDEA. A continuación, se presenta una homologación de estas categorías a la luz de estas normas o modelos que corresponden a buenas prácticas nacionales e internacionales que se han usado para la gestión de documentos electrónicos.

Ciclo de Vida del Documento Electrónico	Componentes del ECM	Moreq2	ISO 15081
1. Producción	**Capturar**	6. Captura e ingreso de documentos	5.5 Captura de datos
5. Organización	**Clasificación e indexación (CCD, tipos documentales, TRD, TVD)**	3. Cuadros de clasificación y organización documental de los expedientes	5.6 Indexación
	Metadatos y taxonomía	12. Gestión de metadatos	5.3.4 Metadatos
4. Trámite	**Gestionar / Administrar**	Flujos de trabajo Workflows / BPM	5.16 Flujos de trabajo

	(Políticas, auditorías)		
	Gestión de documentos		
	Gestión de contenido web		
	Gestión de registros electrónicos		
	Gestión de Email		
	Gestión de activos digitales		
	Colaboración/ Versionamiento		
	Workflow/BPM		
		Flujos electrónicos	5.16 Flujos de trabajo
6. Consulta	**Búsqueda empresarial**	Presentación, recuperación y búsqueda	
3. Distribución	**Distribuir / Entregar**		
8. Disposición final	**Preservar**	5. Retención y disposición	5.9 Retención de documentos
			5.10 Preservación de Información

7. Conservación	**Almacenar**		
	Seguridad	4. Controles y seguridad	5.14 Seguridad y protección
		11. Requerimientos no funcionales	6.5 Revisiones de integridad del sistema

Valor agregado

Como valor agregado, el análisis de las herramientas sugiere la normalización de los procesos de gestión documental y archivo que garanticen y contribuyan a la adecuada creación, tratamiento, conservación, acceso y control de los documentos físicos y electrónicos, por tal motivo se debe adoptar el Cuadro de Actuaciones del Modelo de Gestión de Documentos y Administración de Archivos (MGD), en el cual se condensan líneas de actuación, compromisos por alcanzar para el cumplimiento de dichas líneas de actuación y los diferentes niveles de mejora para la consecución de los compromisos.

A continuación, se relacionan y analizan cada una de las líneas de actuación:

- ✓ Política de Gestión de Documentos y Archivos
- ✓ Gobierno Abierto y Transparencia
- ✓ Administración electrónica
- ✓ Valoración
- ✓ Control intelectual y representación
- ✓ Control de acceso
- ✓ Control físico y conservación
- ✓ Servicios

Capítulo 3
Buenas Prácticas Aplicadas.

Sumario:

3. Buenas Prácticas Aplicadas

3.1 Buenas prácticas en el contexto mexicano

En la reciente Ley General de Archivos en su Libro primero, De la Organización y Administración Homogénea de los Archivos, Título Primero, Disposiciones Generales Artículo 2, se establecen los siguientes numerales:

II. Regular la organización y funcionamiento del sistema institucional de archivos de los sujetos obligados, a fin de que estos se actualicen y permitan la publicación en medios electrónicos de la información relativa a sus indicadores de gestión y al ejercicio de los recursos públicos, así como de aquella que por su contenido sea de interés público;

V. Sentar las bases para el desarrollo y la implementación de un sistema integral de gestión de documentos electrónicos encaminado al establecimiento de gobiernos digitales y abiertos en el ámbito federal, estatal y municipal que beneficien con sus servicios a la ciudadanía;

En ese orden de ideas, en el Capítulo IX, De los documentos de archivo electrónicos, se dice que:

Artículo 42. Los sujetos obligados establecerán en su programa anual los procedimientos para la generación, administración, uso, control y migración de formatos electrónicos, así como planes de preservación y conservación de largo plazo que contemplen la migración, la emulación o cualquier otro método de preservación y conservación de los documentos de archivo electrónicos, apoyándose en las disposiciones emanadas del Consejo Nacional.

Artículo 43. Los sujetos obligados establecerán en el programa anual la estrategia de preservación a largo plazo de los documentos de archivo electrónico y las acciones que garanticen los procesos de gestión documental electrónica.

Los documentos de archivo electrónicos que pertenezcan a series documentales con valor histórico se deberán conservar en sus formatos originales, así como una copia de su representación gráfica o visual, además de todos los metadatos descriptivos.

Artículo 44. Los sujetos obligados adoptarán las medidas de organización, técnicas y tecnológicas para garantizar la recuperación y preservación de los documentos de archivo electrónicos producidos y recibidos que se encuentren en un sistema automatizado para la gestión documental y administración de archivos, bases de datos y correos electrónicos a lo largo de su ciclo vital.

Artículo 45. Los sujetos obligados deberán implementar sistemas automatizados para la gestión documental y administración de archivos que permitan registrar y controlar los procesos señalados en el artículo 12 de esta Ley, los cuales deberán cumplir las especificaciones que para el efecto se emitan.

Las herramientas informáticas de gestión y control para la organización y conservación de documentos de archivo electrónicos que los sujetos obligados desarrollen o adquieran, deberán cumplir los lineamientos que para el efecto se emitan.

Artículo 46. El Consejo Nacional emitirá los lineamientos que establezcan las bases para la creación y uso de sistemas automatizados para la gestión documental y administración de archivos, así como de los repositorios electrónicos, los cuales deberán, como mínimo:

I. Asegurar la accesibilidad e inteligibilidad de los documentos de archivo electrónico en el largo plazo;
II. Aplicar a los documentos de archivo electrónico los instrumentos técnicos que correspondan a los soportes documentales;
III. Preservar los datos que describen contenido y estructura de los documentos de archivo electrónico y su administración a través del tiempo, fomentando la generación, uso, reutilización y distribución de formatos abiertos;
IV. Incorporar las normas y medidas que garanticen la autenticidad, seguridad, integridad y disponibilidad de los documentos de archivo electrónico, así como su control y administración archivística;
V. Establecer los procedimientos para registrar la trazabilidad de las acciones de actualización, respaldo o cualquier otro proceso que afecte el contenido de los documentos de archivo electrónico, y
VI. Permitir adecuaciones y actualizaciones a los sistemas a que se refiere este artículo.

Artículo 47. Los sujetos obligados conservarán los documentos de archivo aun cuando hayan sido digitalizados, en los casos previstos en las disposiciones jurídicas aplicables.

Artículo 48. Los sujetos obligados que, por sus atribuciones, utilicen la firma electrónica avanzada para realizar trámites o proporcionar servicios que impliquen la certificación de identidad del solicitante, generarán documentos de archivo electrónico con validez jurídica de acuerdo con la normativa aplicable y las disposiciones que para el efecto se emitan.

Artículo 49. Los sujetos obligados deberán proteger la validez jurídica de los documentos de archivo electrónico, los sistemas automatizados para la gestión documental y administración de archivos y la firma electrónica avanzada de la obsolescencia tecnológica mediante la actualización, de la infraestructura tecnológica y de sistemas de información que incluyan programas de administración de documentos y archivos, en términos de las disposiciones jurídicas aplicables.

Esta Ley estructura todo un sistema normativo, que de buena forma hace operativo el sistema de archivo electrónico para el Estado mexicano, determinando los elementos y otorgando validez jurídica al documento electrónico.

Así las cosas, en el preámbulo de la Carta Iberoamericana de Gobierno Electrónico, aprobada en 2007, se recogía el compromiso político de reducir la brecha digital y convertir la Sociedad de la Información y el Conocimiento en una oportunidad para todos, especialmente mediante la inclusión de aquellos que corrían el peligro de quedar rezagados. Siguiendo dicho discurso, se recogía la convicción de que el conocimiento constituye un factor esencial de la productividad y el desarrollo humano, por lo que se requerían esfuerzos para evitar las desigualdades, facilitar la inclusión y fortalecer la cohesión social. Y en consonancia con ese sentir, se abordó el alcance del empleo de las TIC por las administraciones públicas, confeccionándose una Carta iberoamericana que contenía conceptos, valores y orientaciones hacia el diseño e implantación de una herramienta que coadyuvara a la mejora de la gestión pública. La "administración electrónica" consiste en la utilización de las TIC en las organizaciones para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y la eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos. En esta misma

línea, la Unión Europea define la administración electrónica como la utilización de las tecnologías de la información y la comunicación en las administraciones públicas, unida a cambios en la propia organización, con el objetivo de mejorar los servicios y los procesos democráticos, y de consolidar el apoyo a políticas públicas. Siguiendo a Jordi Serra (2003), esta administración electrónica focalizará al ciudadano como cliente y se configura como un consumidor de servicios. Esta administración electrónica se fundamenta en unos pilares tecnológicos y otros funcionales. Deteniéndonos en estos últimos, sus principales ejes de actuación serán:

1. Punto único de acceso multicanal, ofreciendo un interlocutor único al ciudadano.
2. Integración de servicios en paquetes, según las necesidades del ciudadano.
3. Tramitación exclusivamente digital de las entradas al sistema, siendo lo digital un factor de integración.
4. Nivel de seguridad superior al presencial, con generación de confianza.
5. Acceso ciudadano a la información de sus trámites.

Propósitos y objeto de la administración electrónica

En el desarrollo y la implantación de la administración electrónica, se reconoce el derecho del ciudadano a relacionarse electrónicamente con las administraciones, lo que implica que las administraciones estén interconectadas permitiendo desarrollar aspectos de interoperabilidad y seguridad de la información que beneficia a los ciudadanos en:

- ✓ Conocimiento y socialización de las labores de la administración.
- ✓ Mayor transparencia y control, generando la confianza de los ciudadanos.

- ✓ Eliminación de barreras de espacio y tiempo, que podían alejar la participación ciudadana.
- ✓ Promoción de la inclusión y la igualdad de oportunidades, con independencia de la situación territorial o social.
- ✓ Participación activa, con la emisión de opiniones, sugerencias y con el seguimiento en la toma de decisiones, así como sobre los servicios y el modo de suministrarlos.

Las posibilidades de relación de los ciudadanos con la administración se extienden a diferentes efectos:

- ✓ Envío de todo tipo de información.
- ✓ Remisión de todo tipo de escritos.
- ✓ Realización de pagos.
- ✓ Recepción de notificaciones.
- ✓ Acceso a información administrativa.
- ✓ Presentación de recursos.

Y ante estas posibilidades de contacto, las administraciones deben adoptar herramientas de respuesta y control para atender adecuadamente el ejercicio efectivo de un derecho:

- ✓ Establecimiento de información accesible al público.
- ✓ Regulación de registros donde se dirijan los ciudadanos.
- ✓ Identificación segura de los ciudadanos.
- ✓ Limitar el régimen de los documentos.

3.2 Referentes legales y normativos del contexto mexicano sobre seguridad de los sistemas de gestión documental electrónica

La gestión de documentos electrónicos se basa en un conjunto de buenas prácticas, estándares y procesos cuya eficiencia en su desempeño depende de la aplicación razonable y sistemática de estos. Para lograr dicho objetivo, es necesario seguir estándares específicos vinculados con la gestión documental.

A escala mundial, hemos avanzado en la estandarización y normatividad clave para incorporar a los sistemas de gestión de las entidades. Entre ellas, hemos tomado y profundizaremos en las normas técnicas internacionales y las normas técnicas homologadas de la Organización Internacional de Normalización, más conocida por su acrónimo en inglés ISO, de gestión de documentos electrónicos y temas de preservación a largo plazo. Estas normas son citadas en el presente ejercicio como referente para evaluar el nivel de madurez y la especificidad técnica requerida para el sistema de gestión de documentos electrónicos y archivos.

Estas normas, como los estándares asociados a gestión electrónica y archivo, han servido como referente a nivel nacional y han sido adoptadas y tomadas para su aplicabilidad en las recomendaciones emitidas por entidades como el Archivo General de la Nación (AGN).

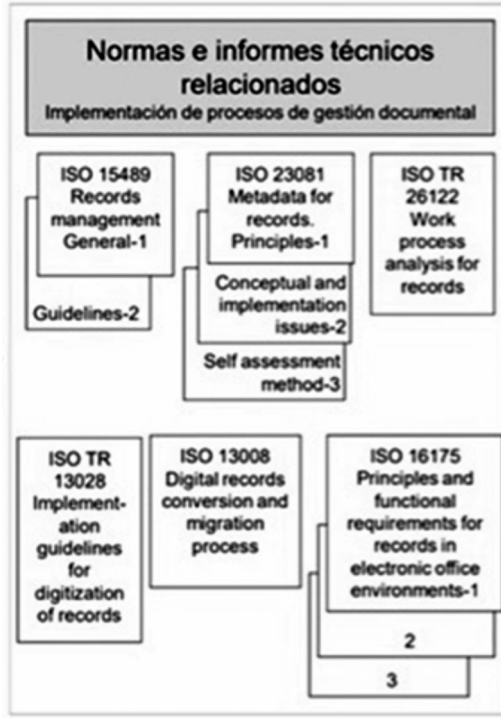
Dentro de las muchas normas ISO que inciden sobre aspectos de gestión, existe un conjunto de normas conocidas como MSS (Management System Standard), que proponen una metodología específica para gestionar las entidades. Esta metodología se basa en los ciclos de mejora continua PHVA, los cuales permiten la definición de objetivos y la elaboración de procedimientos para la medición de los resultados y la

aplicación de medidas correctivas cuando se producen desviaciones sobre lo previsto (no conformidades). Los ejemplos más conocidos y exitosos de estas normas son:

- ✓ La serie 9000 (Sistema de gestión de calidad);
- ✓ La serie 14000 (Sistema de gestión medioambiental);
- ✓ La serie 27000 (Sistema de gestión de seguridad de la información), y
- ✓ La serie de normas ISO 30300 (Sistema de gestión para los documentos que suponen la alineación de las técnicas y los procesos documentales con la metodología de los sistemas de gestión).

No obstante los diferentes significados en idioma español del término documento, es necesario definir previamente a qué nos referimos con “gestión de documentos”. En este caso equivale a lo que en inglés conocemos como récords management o recordkeeping. Las propias normas ISO lo definen como el “área de gestión responsable de un control eficaz y sistemático de la creación, la recepción, el mantenimiento, el uso y la disposición de los documentos, incluidos los procesos para incorporar y mantener, en forma de documentos, la información y prueba de las actividades y operaciones de la organización” (Bustelo-Ruesta, 2012).

Ilustración 2. Normatividad ISO relacionada con gestión de documentos



ISO 30300 / NTC-ISO 30301

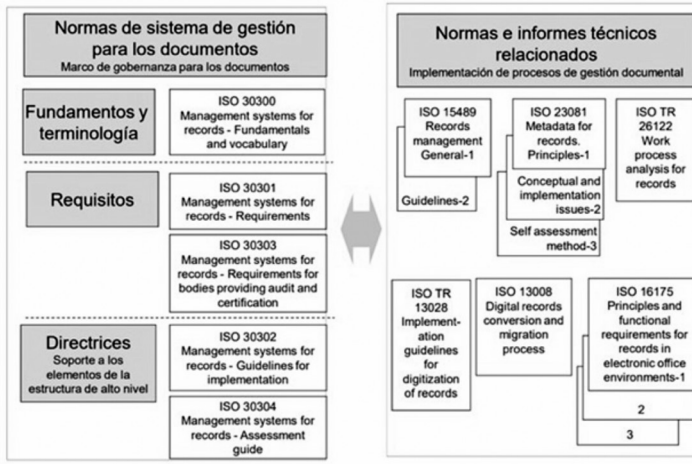
ISO 30300: Información y documentación. Sistemas de Gestión para Registros (SGR). Fundamentos y vocabulario.

Estas normas ofrecen herramientas para la implementación de un sistema de gestión de registros con el fin de crear y gestionar información autorizada y confiable, evidenciar las actividades de la organización, que sean accesibles a quienes las necesitan y el tiempo que se requiera. La

implementación de este sistema ayuda a asegurar la transparencia y trazabilidad de las decisiones tomadas por la gerencia responsable, y al reconocimiento de la rendición de cuentas.

Esta norma fija términos y definiciones aplicables a las normas del sistema de gestión para registros elaborados por el ISO/TC 46/SC 11. También establece los objetivos para el uso de un SGR, brinda los principios para un SGR, describe un enfoque de procesos y específica los roles de la alta dirección.

Ilustración 3. Normatividad ISO relacionada con la ISO 30300



Fuente: ISO 30300.

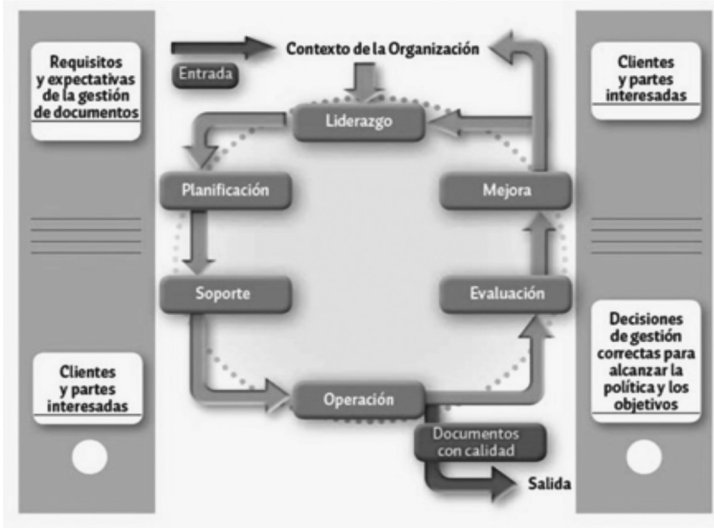
ISO 30301: Información y documentación. Sistemas de Gestión de Registros (SGR). Requisitos.

Sistemas de gestión para los documentos. Creación y control de los documentos durante el tiempo necesario.

El SGR determina los requisitos para la gestión de los registros y las expectativas de las partes interesadas (usuarios y partes interesadas) y, mediante los procesos necesarios, produce registros que satisfacen tales requisitos y expectativas.

Esta norma especifica los requisitos de un SGR con el fin de dar soporte para el cumplimiento de su misión. Se orienta al desarrollo e implementación de una política y objetivos relacionados con los registros y suministra información sobre la medición y el monitoreo del desempeño.

Ilustración 4 Estructura de un Sistema de Gestión de Documentos SGD

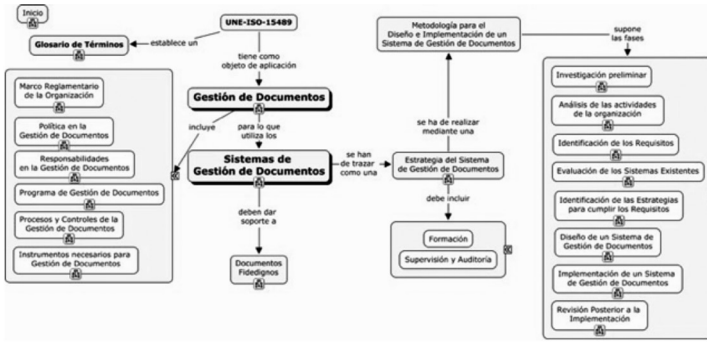


ISO 15489-1: Información y documentación. Gestión de registros. Parte 1: conceptos y principios. Esta norma establece los conceptos esenciales y los principios para la creación, captura y gestión de registros. Describe los conceptos y los principios relacionados con: a) registros, metadatos para registros y sistemas de registros; b) políticas, responsabilidades asignadas, seguimiento y formación para apoyar la gestión eficaz de registros; c) análisis recurrente del contexto de negocio e identificación de los requisitos de los registros; d) controles de registros; e) procesos para la creación, captura y gestión de registros. Esta norma se aplica a la creación, captura y gestión de registros, independientemente de su estructura o forma, en todo tipo de negocios y ambientes tecnológicos a lo largo del tiempo.

La gestión de registros incluye:

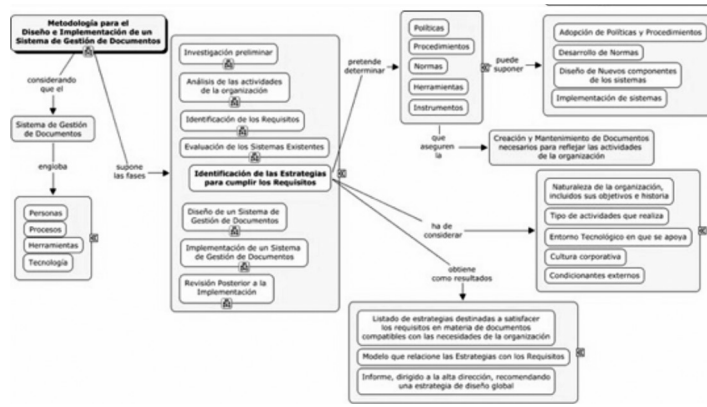
- Crear y capturar registros con el fin de cumplir los requisitos en cuanto a evidencia de la actividad de negocio.
- Tomar las acciones adecuadas para proteger su autenticidad, fiabilidad, integridad y usabilidad en cuanto al contexto de su negocio y a los requisitos para la gestión de cambios a lo largo del tiempo.

Ilustración 5. Mapa descriptivo de la ISO-15489



Fuente: http://cmapspublic3.ihmc.us/rid=1LH3ZC9B6-1WMZMR9-17CG/UNE-ISO-15489-1.cmap

Ilustración 6. Mapa de la metodología para el diseño de un SGD según ISO-15489

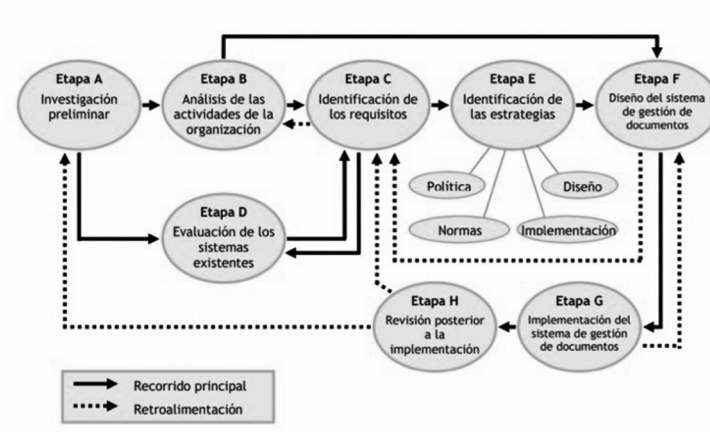


Fuente: http://cmapspublic3.ihmc.us/rid=1LH3ZC9B5-13CMG24-17BN/MetodologiaImplantacionSGD-F5.cmap

GT-ISO-TR-15489-2: Información y documentación. Gestión de documentos. Parte 2: Guía para la implementación de la norma ISO 15489-1.

Proporciona una metodología que facilitará la administración de documentos en cualquier formato o medio. Presenta un panorama de los procesos y factores por considerar en las entidades que desean cumplir con la norma ISO 15489-1. Así pues, a menos que se indique algo diferente, los sistemas se pueden interpretar como papel/sistema manual o electrónico, y un documento puede estar en papel, microforma o electrónico.

Ilustración 7 Diseño e implementación de sistemas de documentos ISO 15489



Fuente: GTC-ISO-TR 15489-2.

GTC-ISO-TR 18492

GTC-ISO-TR-18492: Preservación a largo plazo de la información basada en documentos electrónicos.

Proporciona directrices metodológicas prácticas para la preservación a largo plazo y la recuperación de información auténtica, basada en documentos electrónicos, cuando el período de retención supera la expectativa de vida útil de la tecnología (hardware y software) usada para crear y mantener la información.

Estas directrices también reconocen que para asegurar la preservación a largo plazo y la recuperación de información auténtica basada en documentos electrónicos, se deben involucrar especialistas en tecnologías de la información, administradores de documentos, administradores de registros y archivistas. No se incluyen procesos para crear, capturar ni clasificar información auténtica basada en documentos electrónicos. Esta norma se aplica a todas las formas de información generada por los sistemas de información y que se guarda como evidencia de las transacciones y actividades del negocio.

ISO-IEC 27000 / ISO/IEC 27001

ISO-IEC 27000: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Visión general y vocabulario.

La familia de normas ISO 27000 orientan la implementación del sistema de gestión de la seguridad de la información. De esta gran familia de normas destacamos:

ISO/IEC 27000. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la Información (SGSI). Visión general y vocabulario.

ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la Información (SGSI). Requisitos.

GTC-ISO/IEC 27002. Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información.

GTC-ISO/IEC 27003. Tecnología de la información. Técnicas de seguridad. Guía de implementación de un sistema de gestión de seguridad de la información.

ISO/IEC 27005. Gestión de riesgos de la Seguridad de la Información.

Con el uso de las normas de la familia SGSI, las entidades pueden desarrollar e implementar un marco para gestionar la seguridad de sus activos de información incluyendo información financiera, propiedad intelectual, información personal o información confiada a una organización por usuarios o por terceros.

Esta norma proporciona una visión general de los Sistemas de Gestión de Seguridad de la Información, así como los términos y definiciones de uso común en la familia de normas de SGSI. Esta norma es aplicable a entidades de todo tipo y tamaño (por ejemplo, empresas comerciales, agencias gubernamentales, entidades sin ánimo de lucro).

ISO-IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la Información (SGSI). Requisitos.

Esta norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización.

Asimismo, especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. Incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma son genéricos y están previstos para ser aplicables a todas las entidades, independientemente de su tipo, tamaño o naturaleza.

Ilustración 8. Modelo PHVA aplicado a los procesos de SGSI

Fuente: ISO 27001.

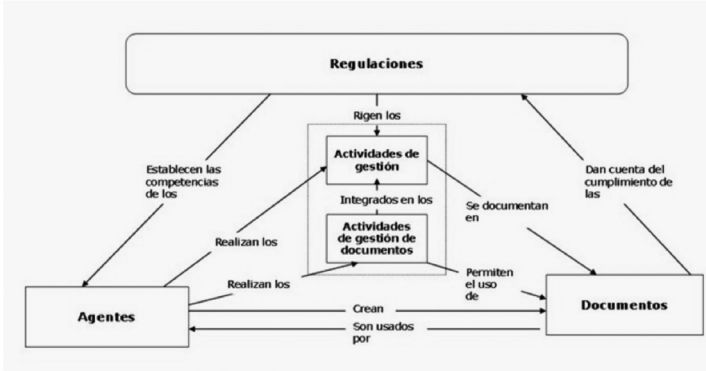
NTC-ISO 23081-1 /NTC-ISO 23081-2

La familia de normas ISO 23081 establecen un marco de referencia para crear, gestionar y usar metadatos para la gestión de registros y explica los principios que lo gobiernan. De esta gran familia de normas destacamos:

NTC-ISO-23081-1: Información y documentación. Procesos para la gestión de registros. Metadatos para los registros. Parte 1: Principios.

Esta norma establece un marco de referencia para crear, gestionar y usar metadatos para la gestión de registros y explica los principios que lo gobiernan. Es una guía para entender, implementar y utilizar metadatos dentro del marco de referencia de la norma ISO 15489. Aborda la relevancia de los metadatos para la gestión de registros en los procesos del negocio y los diferentes roles y tipos de metadatos que sustentan los procesos del negocio y de gestión de registros. También establece un marco de referencia para la gestión de tales metadatos.

Ilustración 9. ISO 23081 – Principales entidades y sus relaciones



ISO 23081-2: Información y documentación. Gestión metadatos para los registros. Parte 2: Aspectos conceptuales y de implementación.

Se enfoca en el marco de referencia para definir los elementos de los metadatos para la gestión de registros y suministra una declaración genérica de los elementos de los metadatos, sean físicos, analógicos o digitales, consistentes con los principios de la ISO 23081-1.

Suministra un fundamento ampliado para los metadatos en la gestión de registros en las entidades, los modelos conceptuales para los metadatos y un conjunto de elementos de alto nivel de tipos de metadatos genéricos adecuados para cualquier entorno de registros que incluya, por ejemplo, documentos actuales, implementaciones para gestión de registros o para archivos. Define los tipos de metadatos genéricos tanto para las entidades de los registros como para otras que es necesario gestionar con el fin de documentar y entender el contexto de los registros.

También identifica, para las entidades claves, un número mínimo de capas de agrupación fijas que se requieren con fines de interoperabilidad. Los modelos y los tipos de metadatos genéricos resumidos en esta parte se centran principalmente en la entidad "registros". Sin embargo, también son pertinentes para otras entidades.

ISO-23081-3: Información y documentación. Gestión metadatos para los registros. Parte 3: Método de autoevaluación.

Esta guía proporciona directrices sobre la ejecución de una autoevaluación en los metadatos de registros con respecto a la creación, la captura y el control de registros. La autoevaluación posibilita: a) identificar el estado actual de la captura y la gestión de metadatos dentro de una organización o entre entidades; b) identificar prioridades sobre en qué trabajar y cuándo; c) identificar los requisitos claves a partir de las normas NTC-ISO 23081-1 y NTC-ISO 23081-2; d) evaluar el avance en el desarrollo de un marco de referencia de metadatos para la implementación de sistemas y proyectos específicos; e) evaluar la disponibilidad de sistemas y proyectos (proseguir hacia la fase siguiente en un sistema o un proyecto) cuando se incluye la funcionalidad de metadatos de registros en un sistema. Se proporciona una evaluación de la disponibilidad de metadatos de registros para las etapas claves desde el inicio del proyecto a través de toda la fase de implementación/mantenimiento.

Norma ISO 14641-1

ISO-14641-1: Archivado electrónico. Parte 1: especificaciones relacionadas con el diseño y el funcionamiento de un sistema de información para la preservación de información electrónica.

Los documentos electrónicos son una parte esencial en el día a día de los negocios, aun si las fuentes son las comunicaciones que llegan o salen de la organización. Es importante que los documentos electrónicos se almacenen correctamente, en su totalidad o en parte, en sistemas de información seguros diseñados para operaciones y archivado, con el fin de satisfacer los requisitos legales, reglamentarios y del negocio.

Esta norma está destinada a brindar un marco de referencia para las entidades. Describe los métodos y las técnicas para implementar un sistema de información electrónica para el manejo de los documentos dentro de un archivo. Junto con las políticas de las entidades relacionadas con el archivo, esta describe criterios para el diseño y las especificaciones del sistema para los procesos operativos.

Esta norma provee un conjunto de especificaciones técnicas y políticas organizacionales que se han de implementar para la captura, el almacenamiento y el acceso a documentos electrónicos. Esto garantiza legibilidad, integridad y trazabilidad de los documentos durante el tiempo de su preservación.

GTC-ISO-TR 15801

GTC-ISO-TR-15801: Gestión de documentos. Información almacenada electrónicamente. Recomendaciones para la integridad y la fiabilidad.

Esta guía define prácticas recomendadas para el almacenamiento electrónico de información de negocios u otra en una forma electrónica. Para las entidades es importante cumplir con sus recomendaciones, incluso cuando no se está poniendo en riesgo la integridad de la información almacenada.

También describe la implementación y la operación de sistemas de gestión de documentos que pueden considerarse para almacenar información electrónica de manera íntegra y fiable. Esta guía es para uso de cualquier organización que utilice un sistema de gestión de documentos para almacenar información electrónica auténtica, fiable y usable/leíble a largo plazo. Tales sistemas incorporan políticas, procedimientos, tecnología y requisitos de auditoría que aseguran que la integridad de la información electrónica se mantiene durante el almacenamiento.

NTC 6231

NTC 6231: Valor probatorio y admisibilidad de la información electrónica. Especificaciones.

Esta norma aborda la manera en que la información necesita ser gestionada por una organización mediante un sistema de gestión de la información, para posibilitar que tenga un valor probatorio fuerte y que su autenticidad e integridad sean confiables y que esto se pueda demostrar siempre que sea necesario durante su ciclo de vida, ya sea para propósitos de negocios, de cumplimiento, legales o para la resolución de conflictos.

Especifica los requisitos para la implementación y la operación de sistemas de gestión de la información electrónica, incluidos el almacenamiento y la transferencia de información, con el objetivo de posibilitar que el usuario asegure que se mantiene la autenticidad e integridad de esta, de manera que sea confiable y aceptada sin objeciones, o que responda adecuadamente a los desafíos cuando se ponga a prueba.

La Norma Técnica Colombiana - NTC 6231 incluye:

- ✓ La gestión de la disponibilidad de la información electrónica con el paso del tiempo.
- ✓ La transferencia electrónica o la comunicación de información electrónica.
- ✓ El vínculo de la identidad electrónica con información electrónica particular; incluido el uso de firmas electrónicas y sistemas electrónicos de derecho de autor, así como la verificación de la identidad electrónica.

Incluye, además, los requisitos para la administración y rendición de cuentas con respecto a la gestión de la información a lo largo de su ciclo de vida.

ISO 14721

ISO 14721: Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia.

Un OAIS es un archivo, que una organización opera, de personas y sistemas que han aceptado la responsabilidad de conservar información y ponerla disponible para una comunidad específica.

Esta norma regula las funciones de preservación de archivos: almacenamiento de archivos, gestión de datos, migración de la información digital a otros formatos, ingesta, acceso y difusión.

Ilustración 10. ISO 14721 – Modelo de referencia

Fuente: Adaptación tomada de la ISO 14721.

ISO 20652

ISO 20652: Datos espaciales y sistemas de transferencia de información - Producer-Archive Interface - Methodology Abstract Standard (PAIMAS).

Esta norma se centra en detallar la relación entre el productor que transfiere el contenido digital y el archivo que asume la responsabilidad de preservarlo, describe el flujo de trabajo de negociar y coordinar las transferencias.

UNE-ISO 19005

UNE-ISO 19005: Formato de fichero de documento electrónico para la conservación a largo plazo.

El objetivo principal de esta norma es definir un formato de archivo basado en PDF, conocido como PDF / A, que proporciona un mecanismo para representar documentos electrónicos de una manera que preserve su aspecto visual estático a lo largo del tiempo. Define los requisitos que conforman un archivo .pdf/a-1.

ISO 32000-1

ISO 32000-1: Gestión de documentos - PDF (sigla del inglés Portable Document Format, "formato de documento portátil").

PDF es un formato de almacenamiento para documentos digitales independiente de plataformas de software o hardware. Este formato es de tipo compuesto (imagen vectorial, mapa de bits y texto). Fue publicado por la Organización Internacional de Estandarización (ISO) como ISO 32000-1.

La norma ISO 32000 cumple los objetivos de proteger la integridad y longevidad del formato PDF, lo que proporciona un estándar abierto para los más de mil millones de archivos PDF que existen hoy en día.

ISO / IEC 29500-1

ISO / IEC 29500-1: Tecnología de la información - Descripción del documento y lenguajes de procesamiento - Formatos de archivo Office Open XML - Parte 1: Fundamentos y referencia del lenguaje de marcado.

Define un conjunto de vocabularios XML para representar documentos de procesamiento de textos, hojas de cálculo y presentaciones. Por un lado, el objetivo de ISO / IEC 29500 es capaz de representar fielmente el corpus preexistente de documentos de procesamiento de textos, hojas de cálculo y presentaciones que han sido producidas por las aplicaciones de Microsoft Office. También especifica los requisitos para los consumidores y productores de Office Open XML. Por otro lado, el objetivo es facilitar la extensibilidad y la interoperabilidad al permitir implementaciones de múltiples proveedores y en diversas plataformas.

ISO/IEC 26300

ISO / IEC 26300: Tecnología de la información - Formato de documento abierto para aplicaciones de Office (OpenDocument) v1.0.

Define un esquema XML para aplicaciones de oficina y su semántica. El esquema es adecuado para documentos de oficina, incluidos documentos de texto, hojas de cálculo, gráficos y documentos gráficos, como dibujos o presentaciones, pero no está restringido a este tipo de documentos. Proporciona información de alto nivel adecuada para la edición de documentos. Define estructuras XML adecuadas para documentos de oficina y es amigable con transformaciones que usan XSLT o herramientas similares basadas en XML.

ISO 16642

ISO 16642: Aplicaciones informáticas en terminología – marco de marcado terminológico.

Especifica un marco diseñado para proporcionar orientación sobre los principios básicos para representar los datos registrados en las colecciones de datos terminológicos. Este marco incluye un metamodelo y métodos para describir los lenguajes de marcado terminológicos (TML) específicos expresados en XML. Define los mecanismos para implementar restricciones en un TML.

Bibliografía

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA. Modelo de requisitos para la implementación de un sistema de gestión de documentos electrónicos. Bogotá: Imprenta Nacional. 2017.

Bustelo Ruesta, Carlota. "La normalización internacional en información y documentación: ¿una historia de éxitos? El caso de la normalización ISO en gestión de documentos" En: Métodos de Información (MEI), II época, vol. 3, núm. 4, 2012, pp. 39-46.

CARTA IBEROAMERICANA DE GOBIERNO ELECTRÓNICO. Adoptada por la XVII Cumbre Iberoamericana de Jefes de Estado y de Gobierno. Santiago de Chile. 2007.

J. Burgos. "Modelo para el Control de Riesgos de Seguridad de la Información en Áreas de Tecnologías de la Información y Comunicaciones (TIC)", Informe de Proyecto de Título, Ing. (E) Computación e Informática, Universidad del Bío-Bío, Concepción, Chile, 2008. Disponible en Biblioteca y/o Departamento de sistemas de información de la Facultad de Ciencias Empresariales.

LEY GENERAL DE ARCHIVOS. Texto vigente a partir del 15-06-2019. Nueva Ley publicada en el Diario Oficial de la Federación el 15 de junio de 2018.

Metodología MAGERIT – Versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Desarrollada por El Consejo Superior de Administración Electrónica del gobierno de España.

ISO 9001. Requisitos de los Sistemas de gestión de la calidad.

ISO 15489. Información y documentación. Gestión documental.

SERRA SERRA, J. 2003. L'administració electrònica i la gestió de documents. BiD: textos universitaris de biblioteconomia i documentació [en línea], 11. [Consulta: 18 septiembre 2019]. Disponible en: http://bid.ub.edu/11serra.htm

UNE-EN ISO 14001. "Sistemas de gestión ambiental. Requisitos con orientación para su uso".

UNE-ISO/TR 18492 IN: Conservación a largo plazo de la información basada en documentos.

UNE-ISO/IEC 27001. Seguridad de la información.

UNE-ISO 30300. Información y documentación. Sistemas de gestión para los documentos.

UNE-ISO 23081. Información y documentación. Procesos de gestión de documentos. Metadatos para la gestión de documentos.

UNE-ISO7TR 26122 IN: Información y documentación. Análisis del proceso de trabajo para la gestión de documentos.

UNE 139803:2012. Requisitos de Accesibilidad para contenidos en la web.

W. E. Deming. “Calidad, Productividad y Competitividad: La Salida de la Crisis”. Ed. Díaz de Santos, España, 1989.

Enlaces de interés

https://www.agesic.gub.uy/innovaportal/v/287/1/agesic/ley-de-documento-electronico-y-de-firma-electronica.html

http://cmapspublic3.ihmc.us/rid=1LH3ZC9B6-1WMZMR9-17CG/UNE-ISO-15489-1.cmap.

http://cmapspublic3.ihmc.us/rid=1LH3ZC9B5-13CMG24-17BN/MetodologiaImplantacionSGD-F5.cmap.

https://www.agci.cl/index.php/centro-de-documentacion2

https://www.boe.es/buscar/pdf/2003/BOE-A-2003-23399-consolidado.pdf