Unitrópico
Universidad Internacional del Trópico Americano

SISTEMA DE GESTIÓN DOCUMENTAL:
Los e-Docs y la Gestión documental durante la pandemia

Por: ghersongrajales@gmail.com

Sesión 04

La preservación documental durante la pandemia pandemia

El patrimonio documental es un recurso importante para ofrecer una perspectiva histórica sobre la forma en que los gobiernos, sus ciudadanos y la comunidad internacional han abordado las pandemias en el pasado.

La preservación documental durante la pandemia.

Se han establecido las siguientes declaraciones para la preservación del patrimonio documental durante la pandemia:

- De la UNESCO del 3 de abril de 2020, Programa Memoria del Mundo.
- Del ICA (Consejo Internacional de Archivos) del 4 de mayo de 2020.

Unitrópico
Universidad Internacional del Trópico Americano

Ambientes de teletrabajo

Unitrópico
Universidad Internacional del Trópico Americano

Ambientes de teletrabajo

Documentos electrónicos (E-Docs)

Documento Electrónico de Archivo es:

un Documento Electrónico que permanece en estos medios electrónicos, ópticos o similares durante su ciclo vital; es producida por una persona o entidad a razón de sus actividades y debe ser tratada conforme a los principios y procesos archivísticos

Documentos electrónicos (E-Docs)

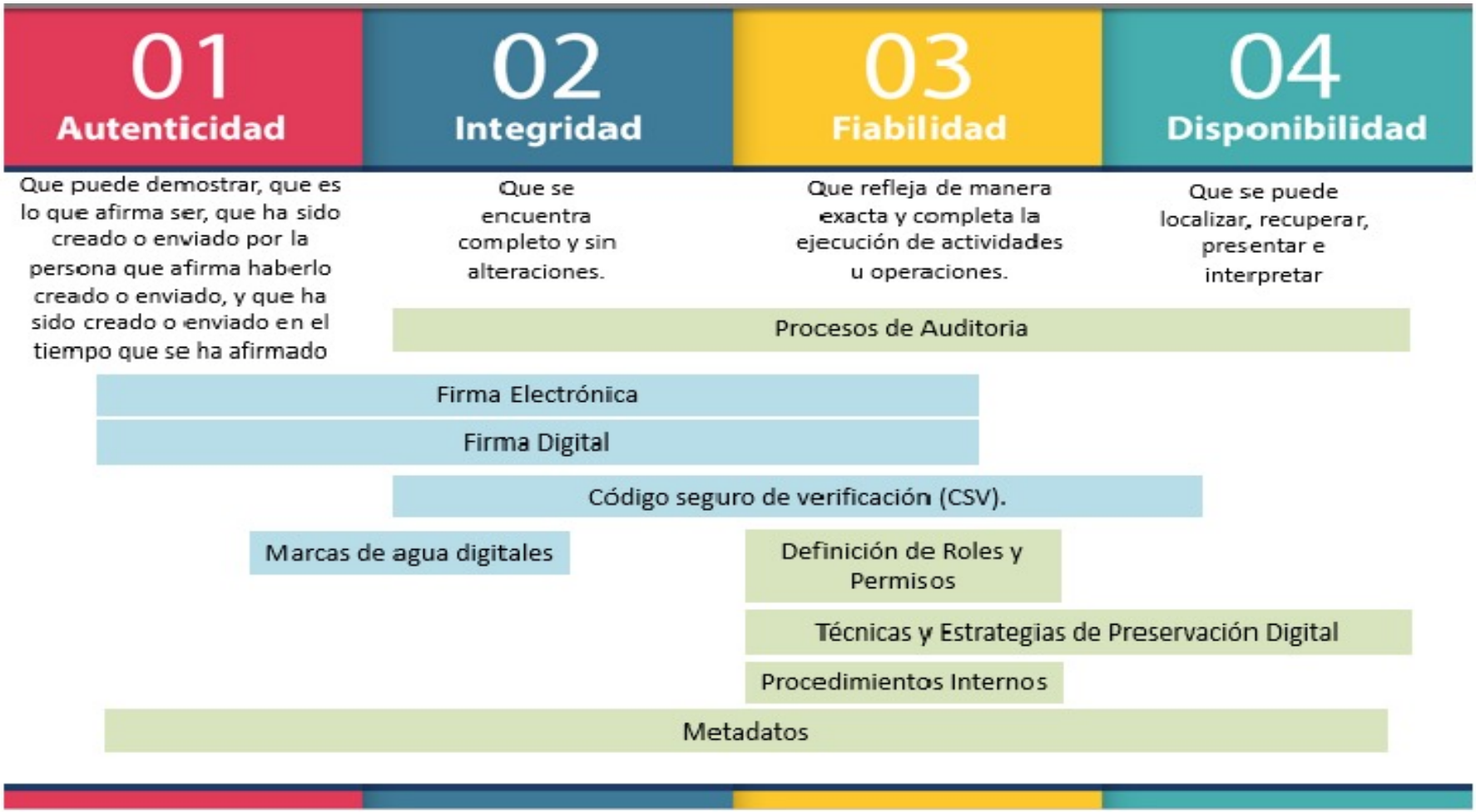
- Información generada, enviada, recibida, almacenada y comunicada por medios electrónicos, ópticos o similares.
- El Código General del Proceso - Ley 1564 de 2012, establece que son documentos los escritos, impresos, planos, dibujos, cuadros, mensajes de datos, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, videograbaciones, 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.

Unitrópico
Universidad Internacional del Trópico Americano

E-Docs: estructura.

Unitrópico
Universidad Internacional del Trópico Americano

E-Docs: características



Unitrópico
Universidad Internacional del Trópico Americano

E-Docs: fiabilidad, integridad y autenticidad.

La confiabilidad en la forma en la que se haya generado.

La confiabilidad en la forma en que se haya archivado.

La confiabilidad en la forma en que se haya comunicado el mensaje.

La confiabilidad en la forma en que se haya conservado.

La integridad de la información.

La forma en la que se identifique a su iniciador.

E-Docs: fiabilidad, integridad y autenticidad.

- Son características esenciales para valorar la fuerza probatoria de un mensajes de datos o un documento electrónico.
- Son características esenciales para el Intercambio Electrónico de Datos (EDI), a través de a transmisión electrónica de datos de una computadora a otra, las cuales están estructuradas bajo normas técnicas convenidas para tal efecto.
- En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y, probatoria a todo tipo de información en forma de mensaje de datos.
- El mensaje de datos debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, debe dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento.

Fiabilidad.

- La capacidad de un documento para asegurar que su contenido es una representación completa, fidedigna y precisa de las operaciones, actividades y hechos que testimonia
- Se puede establecer, declarar o sostener del acto o hecho del que es relativo, determinando la competencia del autor y examinando tanto la completitud en la forma del documento como el nivel de control ejercido durante su proceso de producción.

Fiabilidad.

- Toda organización deberá establecer y documentar el conjunto de reglas que se aplican para elaborar un documento de archivo.
- A mayor estandarización y rigor en el procedimiento, mayor fiabilidad de que el documento de archivo es lo que presume ser.
- El ideal es que cumpla con varios o todos los criterios o requisitos que se señalen sobre la materia.

Fiabilidad: requisitos.

Para la presunción de fiabilidad de los documentos electrónicos de archivo, se deben crear:

- Dando testimonio de la operación o actividad que reflejan, declarando el acto o hecho del que es concerniente.
- Dando testimonio del lugar, estableciendo la competencia del autor.
- Dando certeza de estar completo en la forma del documento de archivo, incluyendo información de control de su producción.
- Manteniendo su identidad inequívoca, es decir los atributos de contexto y procedencia que le son propios, como evidencia electrónica de las transacciones, actividades o hechos a lo largo del tiempo.
- Mediante métodos seguros y verificables.
- Por individuos que dispongan de un conocimiento directo de los hechos o automáticamente por los instrumentos que se usen habitualmente para realizar las operaciones.

Integridad

- La integridad de la información tiene que ver con que el contenido del documento transmitido por vía electrónica sea recibido en su integridad por el destinatario, tarea que puede cumplirse técnicamente utilizando el procedimiento conocido como "sellamiento" del mensaje, mediante el cual aquel se condensa de forma algorítmica y acompaña al mensaje durante la transmisión, siendo recalculado al final de ella en función de las características del mensaje realmente recibido; de modo, pues, que si el mensaje recibido no es exacto al remitido, el sello recalculado no coincidirá con el original y, por tanto, así se detectará que existió un problema en la transmisión y que el destinatario no dispone del mensaje completo.
- Incluso, la tecnología actual permite al emisor establecer si el receptor abrió el buzón de correo electrónico y presumiblemente leyó el mensaje.

Integridad

- Entendida como la cualidad de un documento para estar completo y sin alteraciones, con la cual se asegura que el contenido y atributos están protegidos a lo largo del tiempo.
- Esta característica guarda una estrecha relación con la "inalterabilidad", requisito que demanda que el documento generado por primera vez en su forma definitiva no sea modificado, condición que puede satisfacerse mediante la aplicación de sistemas de protección de la información, tales como la criptografía y las firmas digitales.

Integridad

- Es uno de los componentes que conforman la confianza del documento.
- Se deben establecer medidas de control en el sistema en el que se gestionan o producen los documentos.
- Las medidas de control pueden ser externas al documento electrónico donde se pueda demostrar que la actualización, el mantenimiento habitual o cualquier fallo de funcionamiento del sistema no afectan a la integridad de los mismos.

Integridad: mecanismos de control.

1. Políticas y procedimientos para la administración de bases de datos, documentos electrónicos y demás registros de información.
2. Integridad personal, responsabilidad, confianza del personal que maneja información sensible de la organización.
3. Medidas de protección para evitar la pérdida o corrupción de los documentos de archivo y los medios de almacenamiento.

Integridad: mecanismos de control.

4. Segregación de funciones, es decir asignar y monitorear los permisos de acceso a los datos y documentos electrónicos para que cada función tenga los privilegios que necesita y no abusen de los mismos. Este es un concepto de probada eficacia práctica, en el que seguramente harán hincapié las auditorías internas cuando se revisen sistemas y transacciones de carácter confidencial.

Integridad: mecanismos de control.

5. Integridad en bases de datos, se establece desde la etapa de diseño de una base de datos mediante la aplicación de reglas y procedimientos estándar, y se mantiene a través del uso de rutinas de validación y verificación de errores. Esto incluye integridad de las entidades, la integridad de los dominios y la integridad referencial.

Integridad: técnicas.

1. Controlar los privilegios y derechos de acceso para prevenir cambios no autorizados de la información.
2. Autenticación, cuando se habla de la integridad del origen (Fuente de los datos). Ya que puede afectar a su exactitud, credibilidad y confianza que las personas ponen en la información.
3. Parches de seguridad sobre el sistema operativo y software base para evitar mantener vulnerabilidades que puedan ser aprovechadas para afectar la integridad de los documentos electrónicos de archivo.

Unitrópico
Universidad Internacional del Trópico Americano

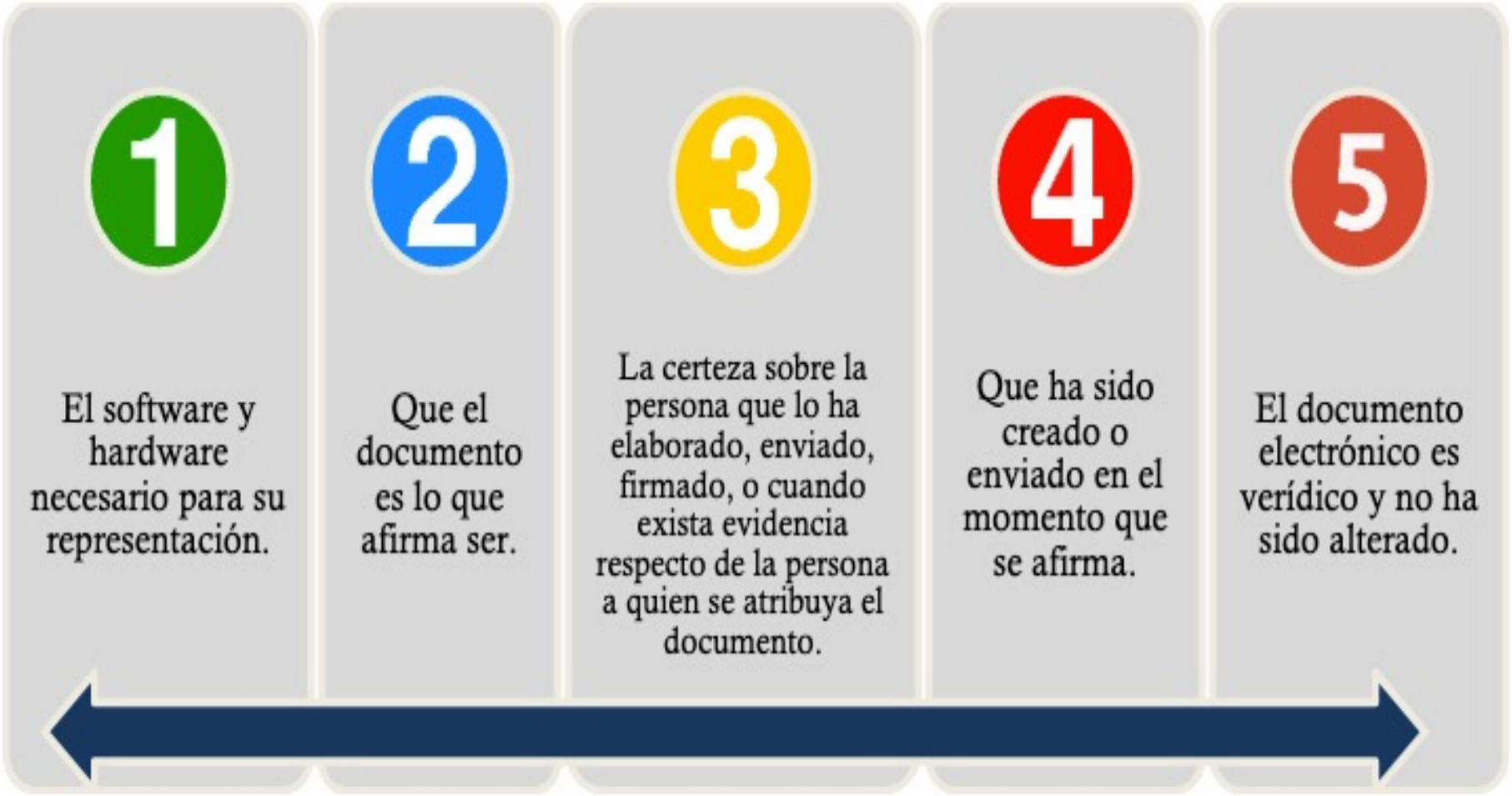
Autenticidad

Autenticidad

- Entendida como el efecto de acreditar que un documento es lo que pretende ser, sin alteraciones o corrupciones con el paso del tiempo.
- Es uno de los componentes que conforman la confianza del documento respecto a su contexto, estructura y contenido.

Unitrópico
Universidad Internacional del Trópico Americano

Autenticidad: identificación.

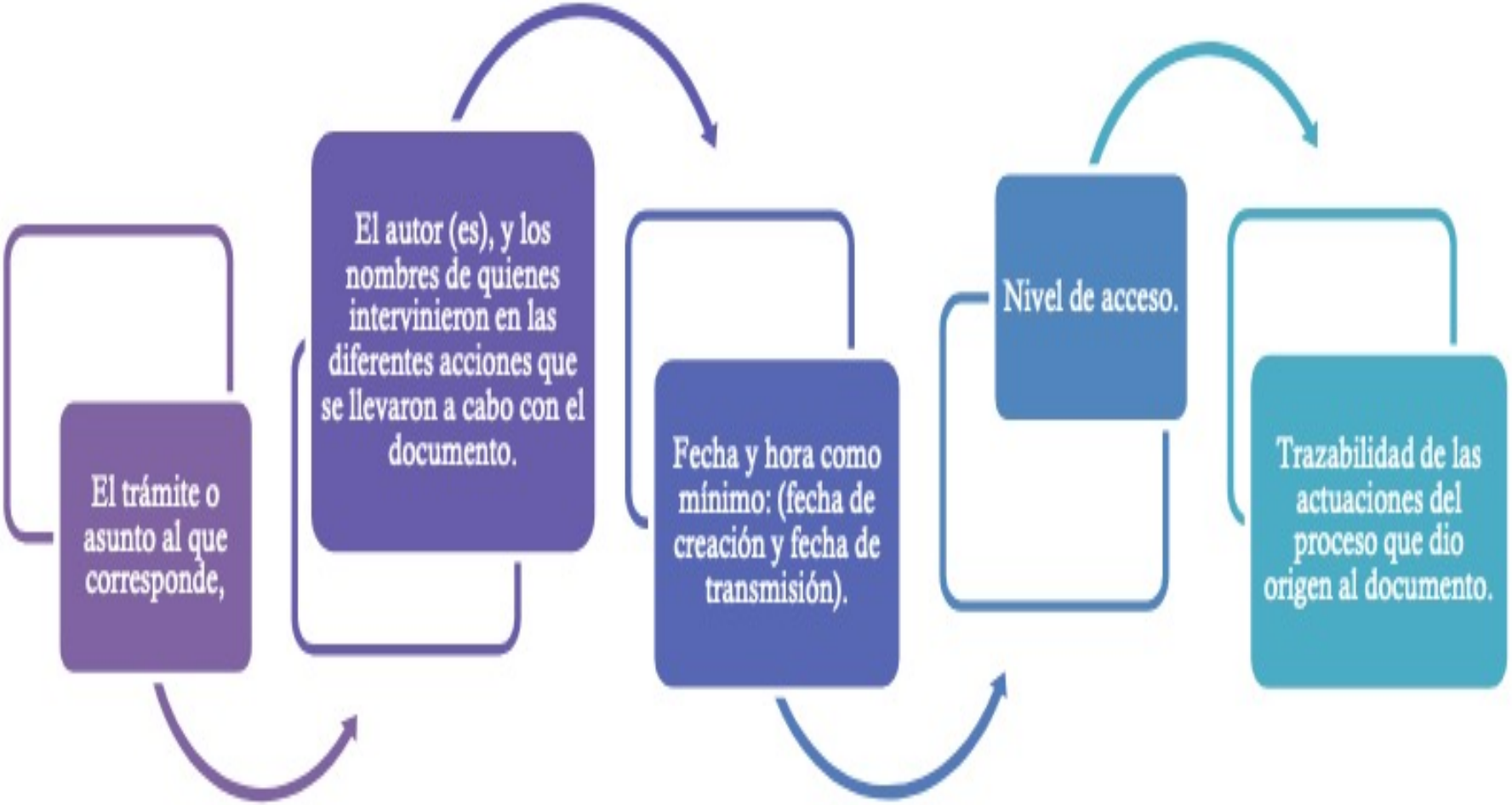


Autenticidad: identificación.

- Se deben documentar e implementar procedimientos de seguridad y control durante todas las etapas del ciclo de vida del documento para evitar la pérdida o corrupción de los documentos de archivo o cualquier adición, supresión, modificación, utilización u ocultación no autorizadas, así como la protección de los medios de almacenamiento y la tecnología.

Unitrópico
Universidad Internacional del Trópico Americano

Autenticidad: metadatos.



Autenticidad: metadatos.

- Para el mantenimiento, modificación, transferencia, preservación y disposición, de los documentos electrónicos de archivo, se debe reflejar la relación o asociación del documento con el expediente a través de la incrustación o vinculación de metadatos.
- Se deberán gestionar metadatos adicionales relacionados con:
  - Nivel de acceso,
  - Privilegios de acceso.

Autenticidad: políticas y procedimientos.

Para asegurar la autenticidad en los documentos electrónicos las entidades deberían establecer políticas y procedimientos:

- a) Para el control de la creación, recepción, transmisión, mantenimiento, disposición y preservación de los documentos electrónicos de archivo, de manera que se asegure que los creadores de los mismos estén autorizados e identificados y que los documentos estén protegidos frente a cualquier adición, supresión, modificación, utilización u ocultación no autorizadas.
- b) Definir procedimientos para asegurar la cadena de preservación o custodia de los documentos electrónicos de archivo a lo largo de su ciclo de vida, y en el transcurso del tiempo.

Autenticidad: técnicas.

Para otorgar autenticidad a los documentos electrónicos las entidades pueden hacer uso de las siguientes técnicas:

a. Estampas de tiempo
b. Firmas electrónicas
c. Firmas digitales
d. Certificados digitales
e. Código seguro de verificación (CSV)
f. Marca de agua digitales

Autenticidad: técnicas.

a) Estampas de tiempo: Consiste en una secuencia de caracteres utilizada para certificar el momento específico en que se lleva a cabo un suceso sobre un documento electrónico o que éste no ha sido modificado en un espacio de tiempo determinado. La secuencia de caracteres está relacionada con la fecha y hora exacta en que ocurre dicho evento y específicamente cuando fue creado o firmado en un sistema de cómputo. Mediante la emisión de una estampa de tiempo es posible garantizar el instante de creación, modificación, recepción, firma, etc., de un determinado mensaje de datos impidiendo su posterior alteración, haciendo uso de la hora legal colombiana.

Autenticidad: técnicas.

b) Firmas electrónicas: 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.

Unitrópico
Universidad Internacional del Trópico Americano

Autenticidad: técnicas.

c) Firmas digitales: La firma digital se configura como un valor numérico que se asocia a un mensaje de datos y permite determinar que dicho valor ha sido generado a partir de la clave originaria, sin modificación posterior. La firma digital se basa en un certificado seguro y permite a una entidad receptora probar la autenticidad del origen y la integridad de los datos recibidos.

Autenticidad: técnicas.

d) **Certificados digitales:** Los certificados digitales se conocen como una parte de la información que se asocia a un mecanismo para acreditar la validez de un documento perteneciente a un autor (autenticación), verificar que no ha sido manipulado ni modificado (integridad), al igual que impide que el autor niegue su autoría (no repudio) mediante validación de la clave pública del autor, quedando de esta manera vinculado al documento de la firma.

Autenticidad: técnicas.

e) **Código seguro de verificación (CSV):** Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente pueden tener la consideración de copias auténticas siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración Pública, órgano o entidad emisora.

Autenticidad: técnicas.

f) **Marcas de agua digitales:** Corresponde a datos incrustados en documentos electrónicos tales como fotografías, películas, audios, y otros contenidos digitales y constituyen un medio seguro para certificar el origen, propiedad y autenticidad de los activos digitales.

Disponibilidad

- Es la capacidad actual y futura de que tanto el documento como sus metadatos asociados puedan ser consultados, localizados, recuperados, presentados, interpretados, legibles, y por tanto estar en condiciones de uso.

Disponibilidad: requisitos.

Para la presunción de disponibilidad de los documentos electrónicos de archivo, se deben tener en cuenta los siguientes requisitos:

1. Cada documento deberá contener la información necesaria para identificar el contexto de las actividades administrativas que lo conforman y el vínculo archivístico, existentes entre los documentos de archivo y el expediente de acuerdo con lo establecido en las Tablas de Retención Documental (TRD).
2. La información debe estar disponible para consulta presente y en el futuro independientemente del sistema que la produjo, su estructura o medio de registro original.
3. Mantener el vínculo permanente entre el documento y sus metadatos.
4. Los documentos electrónicos y la información en ellos contenida, debe estar disponible en cualquier momento, mientras la entidad está obligada a conservarla, de acuerdo con lo establecido en las Tablas de Retención Documental (TRD).

Disponibilidad: mecanismos de control.

- Para garantizar la disponibilidad en los documentos electrónicos las entidades deberían establecer políticas y procedimientos como los siguientes:

1. Plan de respuesta a incidentes y plan de continuidad del negocio.

2. Acuerdos de Niveles de Servicio. La entidad debe velar por la óptima prestación de los servicios de TI "Tecnologías de la información", identificando las capacidades actuales de los Servicios Tecnológicos y proyectando las capacidades futuras requeridas para que cumplan con los niveles de servicio acordados con los usuarios.

Disponibilidad: mecanismos de control.

3. Gestionar la capacidad, la operación y el soporte de los servicios tecnológicos, con criterios de calidad, seguridad, disponibilidad, continuidad, adaptabilidad, estandarización y eficiencia.

4. Prevención de ataques de denegación del servicio: configuración de routers y firewalls para filtrar IPs inválidas, así como el filtrado de protocolos que no sean necesarios. Es recomendado contar con **S**istemas de **D**etección (IDS) o **P**revención (IPS) de **I**ntrusos

Disponibilidad: mecanismos de control.

5. Sistemas de contingencia alternativos o manuales. De esa forma, si la tecnología principal falla parcial o totalmente, habrá un sistema de respaldo que pueda ser puesto en operación.

6. Debe implementar capacidades de alta disponibilidad que incluyan balanceo de carga y redundancia para los Servicios Tecnológicos que afecten la continuidad del servicio de la institución, las cuales deben ser puestas a prueba periódicamente.

Disponibilidad: mecanismos de control.

7. Debe implementar controles de seguridad para gestionar los riesgos asociados al acceso, trazabilidad, modificación o pérdida de información que atenten contra la disponibilidad, integridad y confidencialidad de la información.

Unitrópico
Universidad Internacional del Trópico Americano

Correos electrónicos

Unitrópico
Universidad Internacional del Trópico Americano

Correos electrónicos

Correos a incluir	Correos a descartar
Aquellos cuyo contenido inicia, autoriza o finaliza una acción en una Entidad Distrital	Aquellos con mensajes de carácter personal que no tienen relación con las actividades de la Entidad Distrital.
Aquellos intercambiados entre funcionarios de la Entidad Distrital relacionados con sus actividades que representen registros dentro del sistema de calidad o que estén incluidos dentro de la TRD o que revistan una importancia vital dentro de un trámite.	Aquellos con publicidad, cadenas o cualquier otro tipo de información que no tenga relación con asuntos administrativos.
Aquellos intercambiados con personas naturales o jurídicas en desarrollo de trámites o actividades de la entidad.	Aquellos remitidos como copias a personas o grupos de trabajo con la finalidad de referenciar o enterar sobre algún asunto.
Aquellos cuyo contenido se refiere a registro de reuniones o mesas de trabajo, por ejemplo: invitaciones, orden del día, etc.	Aquellos a través de los cuales se remita material bibliográfico, hemerográfico, normativo, etc. como apoyo teórico o técnico en una actividad.
Aquellos cuyo contenido es nota, informe final o recomendación para una acción en desarrollo o finalizada.	

Documentos digitalizados

Consulta: cuando sirve para permitir el acceso a la información.

Trámite: cuando sirve de apoyo a la gestión administrativa. Incorporara técnicas estándares y procedimientos que permiten garantizar las características de autenticidad, integridad y disponibilidad.

Como medida de seguridad, ya sea con fines de *backup* o contingencia, para lo cual se deberán analizar y determinar los aspectos jurídicos y técnicos para cuando se refiera a una copia exacta de los documentos originales, como por ejemplo el establecimiento de un procedimiento de digitalización certificada.

Documentos digitalizados

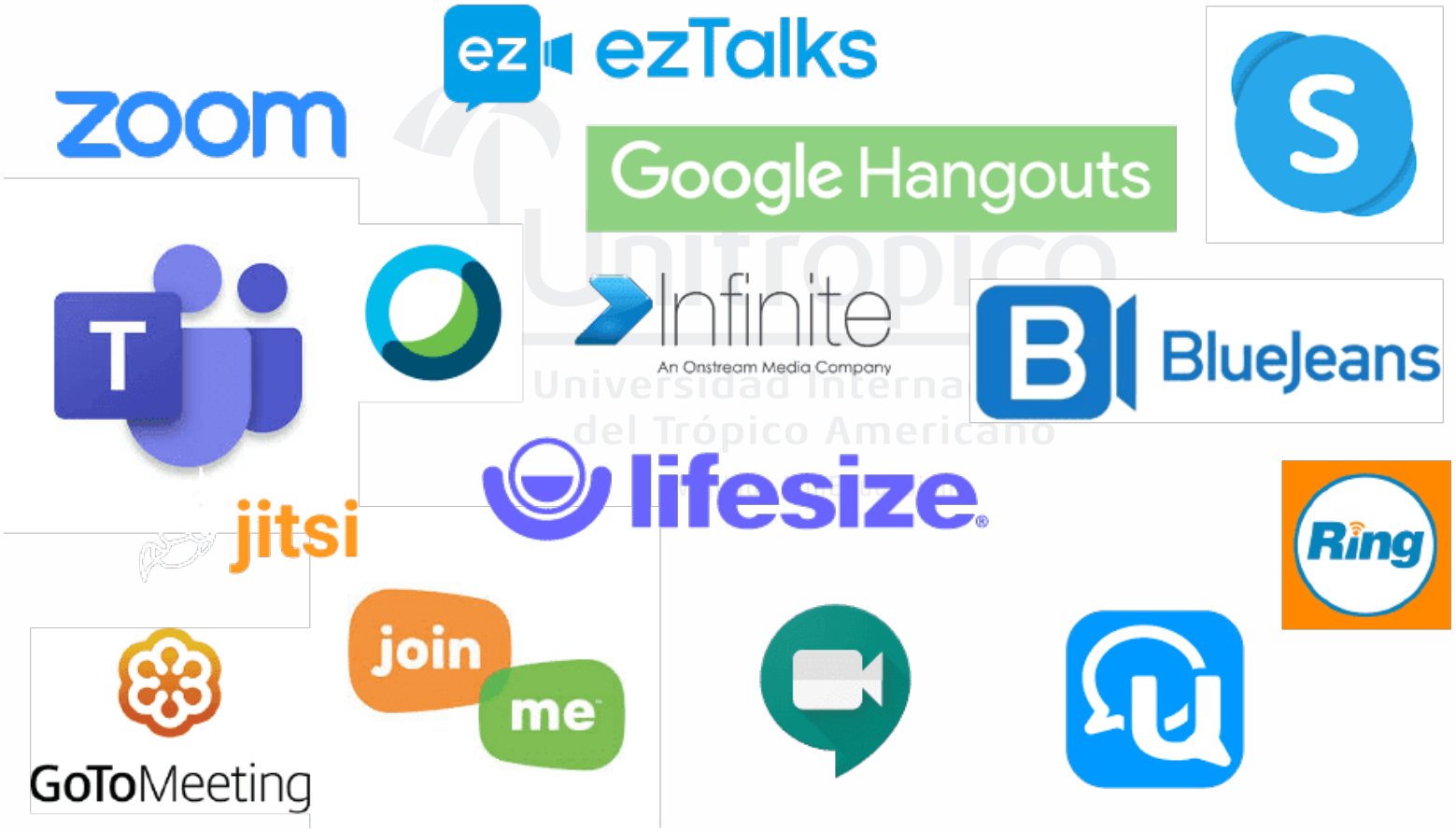
- Es la representación digital, obtenida a partir de un documento registrado en un medio o soporte físico, mediante un proceso de digitalización.
- Se puede considerar como una forma de producción de documentos electrónicos.
- La digitalización en ningún caso podrán aumentar o disminuir los tiempos de retención documental establecido en las Tablas de Retención Documental – TRD.

Documentos digitalizados

- La digitalización de documentos de ninguna manera implica la eliminación o "destrucción" física de los originales.
- Los documentos originales que posean valores históricos NO podrán ser destruidos, aun cuando hayan sido reproducidos y/o almacenados mediante cualquier medio.
- Aún existen documentos que no poseen un equivalente funcional, en cumplimiento estricto de los términos legales, tales como la escritura pública, por cuanto el documento original y físico de estos deberán recibir un trato especial, desde el momento de su emisión hasta que culmine su ciclo de vida, mientras la legislación nacional evoluciona e incorpora este tipo de documentos al mundo digital.

Unitrópico
Universidad Internacional del Trópico Americano

Plataformas de comunicación por Internet



Unitrópico
Universidad Internacional del Trópico Americano

Ventanillas electrónicas

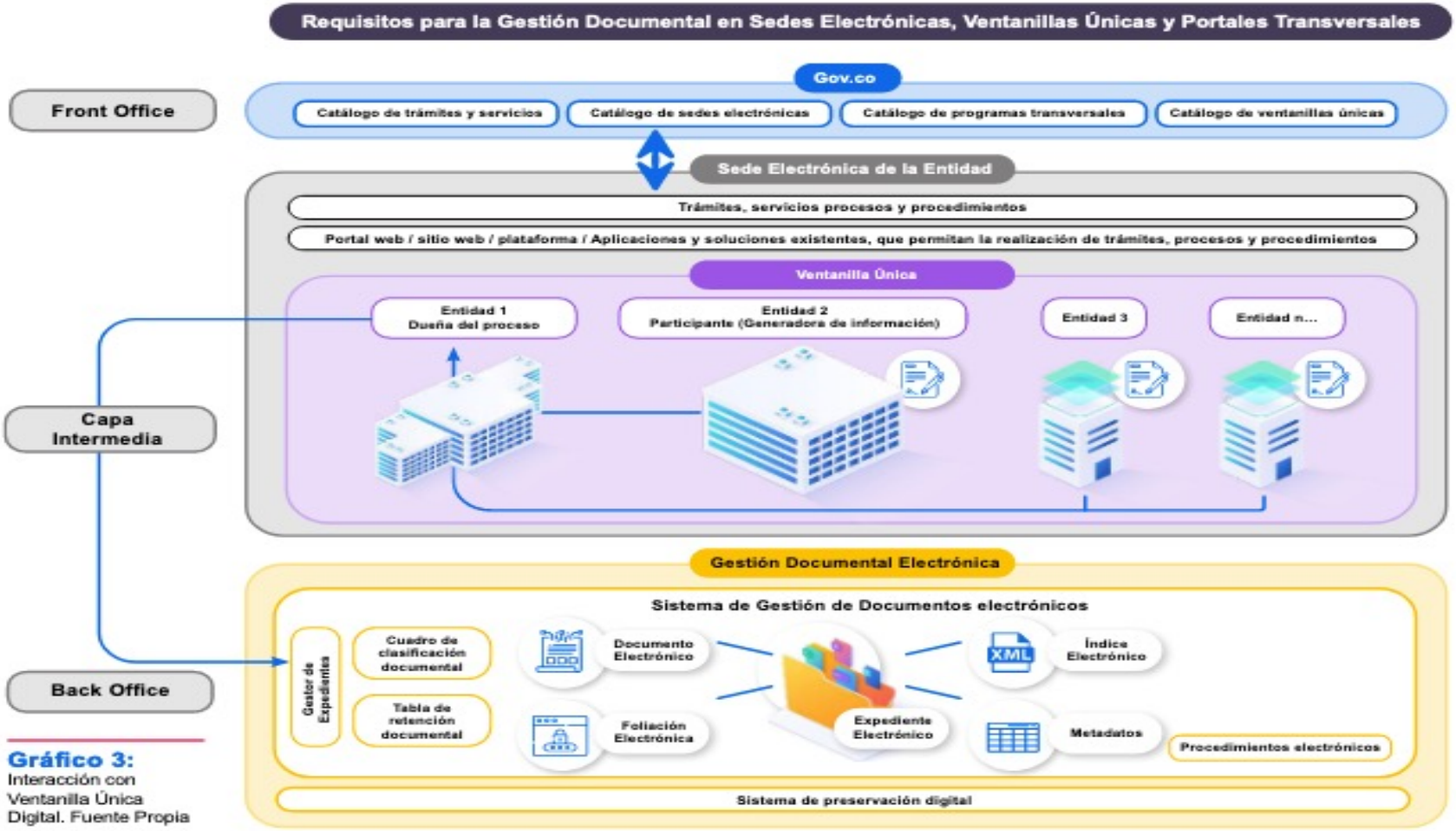
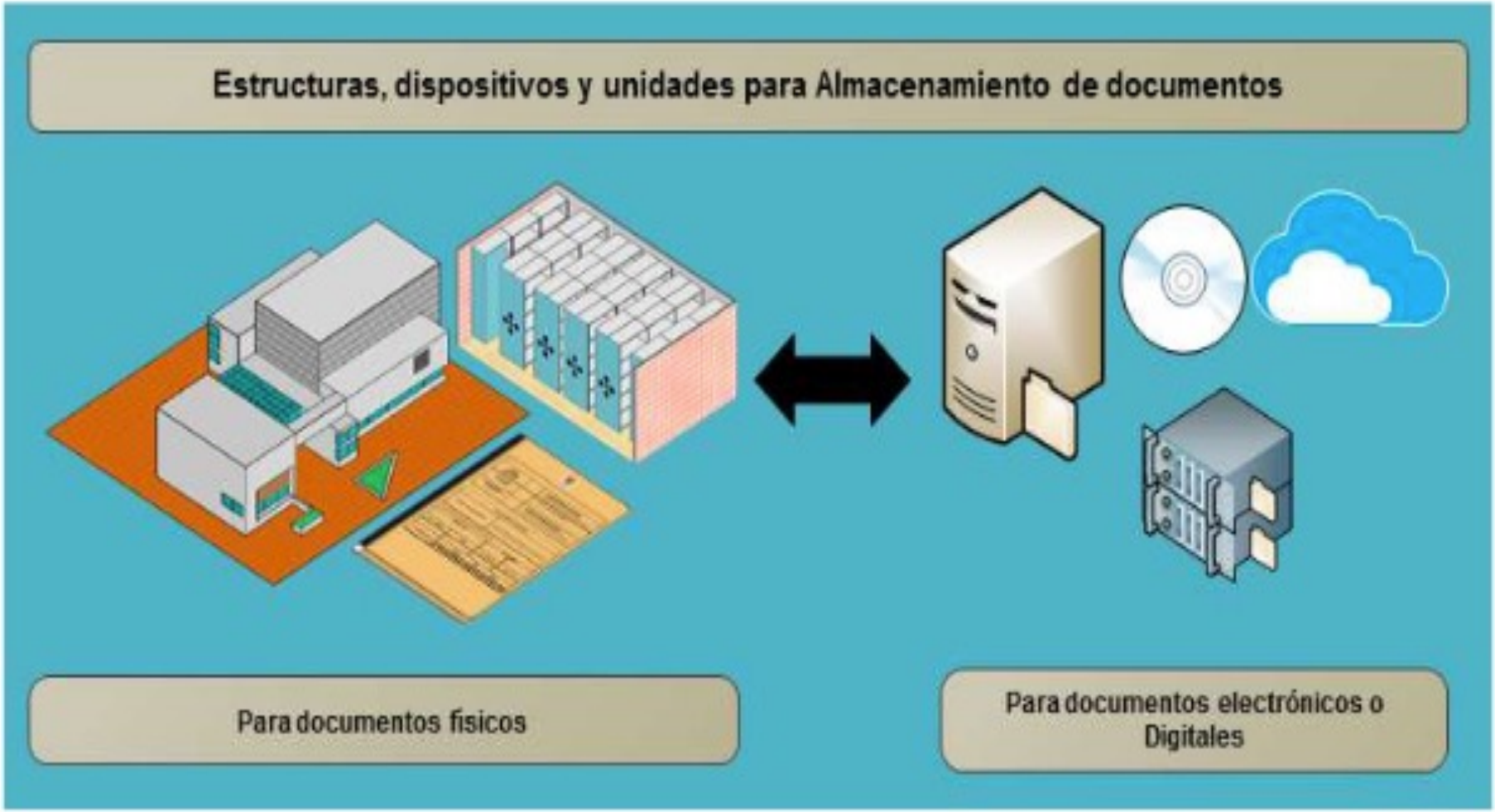


Gráfico 3: Interacción con Ventanilla Única Digital. Fuente Propia

Unitrópico
Universidad Internacional del Trópico Americano

Almacenamiento de documentos electrónicos



Unitrópico
Universidad Internacional del Trópico Americano

GRACIAS