MÓDULO 7: Gestión y preservación de documentos digitales

SECCIÓN 11

GESTIÓN DE UN PROYECTO DE ARCHIVO DIGITAL

IBERARCHIVOS
IBERARQUIVOS

ARCHIVO NACIONAL
COSTA RICA

UNIVERSIDAD DE
COSTA RICA

MÓDULO 7

Gestión y preservación de documentos digitales

SECCIÓN 11

Gestión de un proyecto de archivo digital

Adaptación del Archivo Nacional de Costa Rica
Versión 1, 2024

Este curso fue traducido y adaptado por la Dirección General del Archivo Nacional de Costa Rica en colaboración con la Sección de Archivística de la Universidad de Costa Rica a partir del material original del año 2011 de la Asociación Internacional de Archivos Francófonos disponible en línea en el Portal Internacional Archivístico Francófono. Se aclara que pueden existir variaciones respecto al contenido original. Para acceder al material en francés, visite https://www.piaf-archives.org/se-former/module-7-gestion-et-archivage-des-documents-numeriques.

IBERARCHIVOS IBERARQUIVOS

ARCHIVO NACIONAL COSTA RICA

UNIVERSIDAD DE COSTA RICA

Contenido

Capítulo 1. Objetivo de la sección

Este apartado se refiere a la gestión de un proyecto de archivo electrónico que, como todos los proyectos relacionados con la implementación de un sistema de información, debe ir acompañado de una reflexión sobre la gestión de riesgos y control de costes, antes del lanzamiento real del proyecto.

Además, cualquier proyecto de archivo electrónico debe ir acompañado del desarrollo de una política de archivo, especificando los roles y responsabilidades de los distintos actores y articulándose en una política de seguridad a implementar, que se encuadre en la política general de seguridad de la organización.

GLOSARIO

Acceso a la información: Proceso de consulta y recuperación de la información archivada.

Administradores: Personas responsables de la administración y configuración del sistema de archivo electrónico.

Aspectos Administrativos: Los aspectos de un proyecto que se relacionan con su gestión, planificación y control.

Aspectos Funcionales: Los aspectos de un proyecto que se relacionan con su propósito o funcionalidad previstos.

Aspectos Técnicos: Los aspectos de un proyecto que se relacionan con su tecnología o infraestructura.

Autoridad de archivo: Entidad responsable de la gestión, tratamiento, conservación y comunicación de los datos.

Clasificación de Riesgos: El proceso de categorizar riesgos en función de su probabilidad e impacto.

Contrato o acuerdo: Documento que define el alcance de los datos a transferir/eliminar, así como los procesos de transferencia y eliminación entre los diferentes actores del proceso.

Criticidad: El nivel de importancia de un riesgo, basado en su probabilidad e impacto.

Departamento de archivos: Unidad responsable de la custodia y conservación de los datos una vez que han pasado su fase activa.

Habilidades y Conocimientos Comerciales: La capacidad de comprender y aplicar principios y prácticas comerciales.

Identificación de Riesgos: El primer paso en la gestión de riesgos, que implica identificar posibles riesgos para un proyecto.

Índice de Prioridad de Riesgos (RPI): Un valor numérico que representa la criticidad de un riesgo.

Departamento de producción: Unidad responsable de la creación y gestión de los datos durante su fase activa.

Departamento de TI: Unidad responsable de brindar soporte técnico y tecnológico a los departamentos de producción y archivos.

Especialista: Un individuo con experiencia en un campo particular, como la gestión documental o la gestión de riesgos.

Evaluación de Riesgos: El proceso de evaluar la probabilidad y el impacto de cada riesgo identificado.

FMEA (Análisis de Modos y Efectos de Fallas): Un método para identificar y analizar fallas potenciales en un sistema o proceso.

Gerente de Calidad: Un individuo responsable de garantizar que la calidad de un proyecto cumpla con los estándares requeridos.

Gestión de Riesgos: El proceso de identificar, evaluar y priorizar riesgos en proyectos de gestión documental electrónica para desarrollar e implementar estrategias de mitigación.

Grupo de Trabajo: Un equipo de personas responsables de una tarea o proyecto específico.

Mitigación: Las acciones tomadas para reducir la probabilidad o el impacto de un riesgo.

Modelo OAIS: Modelo de referencia para la gestión de archivos que define los ocho componentes funcionales de un sistema de archivo electrónico.

Norma ISO14721: Estándar que detalla el modelo de referencia OAIS y proporciona pautas para la implementación de sistemas de archivo electrónico.

Norma ISO20652: 2006: Estándar abstracto de metodología de interfaz de archivo de productor que establece los principios generales para la interacción entre el servicio de depósito y el servicio de archivo electrónico.

Política de archivo: Documento que establece las normas y procedimientos para la gestión de archivos dentro de una organización.

Priorización de Riesgos: El proceso de clasificar riesgos en función de su criticidad.

Usuarios: Personas que acceden y utilizan la información archivada.

Capítulo 2. Gestión de riesgos

La preservación de documentos digitales implica un conjunto de acciones preventivas, es ante todo un proyecto como cualquier otro y es fundamental para asegurar la eficiencia y la eficacia en el acceso a la información indistintamente del tiempo que esta deba ser conservada.

El riego de pérdida de información puede conllevar consecuencias graves para las personas, por ejemplo:

- ¿Qué pasaría con un sistema judicial que no ha podido conservar todos los documentos necesarios para la correcta realización de un juicio?
- ¿Qué pasaría con un sistema de salud que ha perdido el rastro de los análisis, exámenes y radiografías previos de un paciente?
- Si las secuelas de un accidente de tráfico aparecen diez o veinte años después de este accidente, ¿qué pensaría de una compañía de seguros que no ha podido preservar su expediente?
- ¿Qué pasaría con una gran agencia científica que realiza proyectos sobre la base de la financiación pública y que no ha podido conservar los datos resultantes de estos proyectos?

Por lo tanto, es responsabilidad de los líderes de esta organización tener en cuenta el problema de la sostenibilidad de la información digital. En este contexto, la gestión de riesgos es fundamental porque proporciona un punto de

referencia sobre el cual basar el desarrollo de acuerdos de servicio entre productores y el servicio de archivo para la transferencia de responsabilidades. Asimismo, deben asegurar que el compromiso del Archivo en términos de conservación y acceso sea proporcional a los riesgos que pesan sobre los documentos y deben definir las condiciones para una misión continua de seguimiento y vigilancia de riesgos, que es definida en el modelo OAIS como «planificación de la sostenibilidad«

No tener en cuenta el problema conduce en última instancia a la pérdida de información que puede ser valiosa, incluso esencial para el funcionamiento de la organización. En el mejor de los casos, la reconstrucción de la información perdida será necesaria y requerirá recursos considerables.

2.1. Metodología y principios

Identificación y clasificación de riesgos

El primer paso crucial en la gestión de riesgos de proyectos de gestión documental electrónica es la identificación y clasificación de los riesgos potenciales. Para ello, se recomienda establecer uno o más grupos de trabajo conformados por “especialistas” o, al menos, por personas con las habilidades y conocimientos comerciales relevantes. Estos grupos serán responsables de elaborar una lista exhaustiva de riesgos, considerando aspectos tanto funcionales como técnicos y administrativos. La participación de un responsable de calidad, cuando sea posible, aportará un valor significativo en cuanto al rigor y la eficacia del proceso.

Evaluación de riesgos

Una vez identificados los riesgos, se debe proceder a su evaluación. Para este paso, se puede utilizar el enfoque FMEA (Análisis de Modos de Falla, Efectos y Criticidad), que permite analizar los diferentes tipos de riesgos, sus posibles efectos y su nivel de criticidad.

Priorización de riesgos

A partir de la evaluación de riesgos, se pueden identificar los riesgos prioritarios. Para ello, se puede establecer un umbral para el Índice de Prioridad de Riesgo (RPI). Los riesgos que superen este umbral requerirán un mayor esfuerzo de control y mitigación.

2.2. Metodología y principios: segunda etapa

Por otra parte, la gestión de riesgos puede ser abordada a partir de la siguiente metodología:

Evaluación de riesgos: según su grado de probabilidad (5 niveles de “improbable” a “frecuente”), su impacto (siempre 5 niveles de “insignificante” a “catastrófico”) y su grado de ocurrencia en el tiempo (de “distante” a “inminente” “).

Toma de decisiones: ¿Son aceptables los riesgos? Según los objetivos de la organización, según el tipo de productores y categorías de usuarios, según los costos y beneficios de las operaciones de control de riesgos, según las obligaciones legales.

Acciones son las medidas que deben tomarse para contener el riesgo:

- que reducen la probabilidad de un riesgo (elija formatos abiertos, por ejemplo),
- que reducen el impacto de un riesgo (por ejemplo, tener un plan de respaldo),

- lo que evita el riesgo (no nos hacemos cargo de los objetos de archivo cuya conservación resulta demasiado arriesgada).

Asimismo, son admisibles otras dos categorías de acciones:

- riesgo compartido: se suscriben pólizas de seguro con terceros contra violaciones de la información y daños inmateriales, como la destrucción voluntaria o involuntaria de datos, la divulgación de información, la calidad inadecuada del programa,
- tolerancia al riesgo: por ejemplo, decidimos asumir el riesgo y pagar una compensación en lugar de garantizar la preservación a largo plazo de algunos de los recursos digitales que conservamos.

Una iteración es esencial para verificar que los controles implementados no han creado otros riesgos, o adaptar la evaluación de riesgos cuando se modifica el sistema o tener en cuenta la evolución de los riesgos.

COMPLEMENTO: EL ENFOQUE DE ANÁLISIS DE MODOS DE FALLA, EFECTOS (FMEA)

El FMEA (Análisis de Modos de Falla y Efectos) ofrece un enfoque deductivo y exhaustivo para la identificación y evaluación de los riesgos que pueden afectar a un sistema. Este método se basa en tres pilares fundamentales:

1. Búsqueda de las causas de fallo: Se realiza un análisis exhaustivo para identificar todas las posibles causas que podrían provocar un fallo en el sistema.
2. Búsqueda de los mecanismos de detección: Se evalúan los mecanismos existentes para detectar las causas de fallo antes de que se produzca un impacto significativo.
3. Búsqueda de recomendaciones: Se proponen medidas para reducir o eliminar las causas de fallo o su impacto en el sistema.

Clasificación de riesgos mediante la criticidad:

El FMEA incorpora el concepto de criticidad para clasificar y priorizar los riesgos identificados. Para ello, se pueden utilizar diferentes métodos, dos de los cuales son:

1. Multiplicación de la gravedad y la aparición:

- Índice de gravedad: Se evalúa la severidad del impacto potencial de un fallo en el sistema.
- Índice de aparición: Se estima la probabilidad de que ocurra la causa de un fallo.

El Índice de Prioridad de Riesgo (RPI) se calcula multiplicando el índice de gravedad por el índice de aparición. Un RPI superior a un umbral predefinido indica la necesidad de implementar medidas para reducir la criticidad del riesgo.

2. Multiplicación de la gravedad, la ocurrencia y la detección:

- Índice de ocurrencia: Se estima la frecuencia con la que se presenta la causa de un fallo.
- Índice de detección: Se evalúa la eficacia de los mecanismos existentes para detectar la causa de un fallo antes de que se materialice.

El RPI se calcula multiplicando el índice de gravedad por el índice de ocurrencia y el índice de detección. Un RPI elevado indica la necesidad de implementar medidas para reducir la probabilidad de ocurrencia o mejorar la detección del riesgo.

Ejemplo de aplicación:

Consideremos el riesgo de degradación de los soportes en una grabación realizada en un CD-R, siguiendo las recomendaciones vigentes.

- Índice de gravedad: Se estima como «grave» (4) ya que existe una copia de seguridad.
- Índice de ocurrencia: Se estima como «moderadamente frecuente» (3) debido a la vida útil limitada del CD-R (3 a 5 años).
- Índice de detección: Se estima como «máximo» (5) debido a la falta de mecanismos de control.

El RPI se calcula como 60 (IPR = 4 x 3 x 5). Este valor indica que es fundamental implementar medidas para detectar la degradación de los CD-R y mitigar el riesgo asociado.

En resumen, el FMEA es una herramienta valiosa para la gestión de riesgos en proyectos de gestión documental electrónica. Su enfoque deductivo y exhaustivo permite identificar, evaluar y clasificar los riesgos de forma sistemática, facilitando la toma de decisiones para su control y mitigación.

COMPLEMENTO: EL MÉTODO “ISHIKAWA”

Definición y origen:

El método Ishikawa, también conocido como diagrama de espina de pescado, es una herramienta gráfica utilizada en la gestión de la calidad para identificar y analizar las causas de un efecto o problema específico. La forma del diagrama, similar a la de una espina de pescado, le da su nombre característico.

Objetivo:

El objetivo principal del método Ishikawa es encontrar todas las posibles causas que contribuyen a un efecto o problema determinado. Esto se logra mediante la lluvia de ideas y la exploración de diferentes dimensiones del problema.

Funcionamiento:

El método se basa en la creación de un diagrama donde:

- El eje central: Representa el efecto o problema que se desea analizar.
- Las ramas principales: Representan las diferentes dimensiones o categorías de causas que pueden estar involucradas.
- Las subramas: Representan las causas específicas dentro de cada categoría.

Las 5M de Ishikawa:

La versión original del método, desarrollada por Kaoru Ishikawa, propone cinco categorías principales, conocidas como las "5M":

- Materia: Materiales y componentes utilizados en el proceso.
- Material: Equipos, herramientas e instalaciones involucradas.
- Método: Procedimientos, instrucciones y técnicas empleados.
- Medio: Entorno de trabajo y condiciones ambientales.
- Mano de obra: Personas involucradas en el proceso, incluyendo sus habilidades y experiencia.

Adaptaciones y variaciones:

Es importante mencionar que existen variaciones del método Ishikawa que han sido adaptadas a diferentes sectores de actividad. Estas variaciones pueden incluir otras categorías o dimensiones específicas relevantes para el sector en cuestión.

2.3. Clasificación de riesgos

Los riesgos pueden ser clasificados de la siguiente manera:

Riesgos ambientales

Los riesgos ambientales son aquellos que provienen del entorno del archivo y se pueden dividir en tres categorías:

- Riesgos naturales: Eventos naturales como terremotos, inundaciones o incendios que pueden afectar el archivo.
- Riesgos de seguridad: Amenazas a la seguridad física del archivo, como robos o intrusiones.
- Riesgos relacionados con el entorno: incluye fallas en el edificio o el hardware necesario para los sistemas informáticos del archivo, así como cortes de energía o fallos del sistema de climatización. En su determinación es importante tomar en cuenta las características particulares de la ubicación geográfica de las instalaciones ya que influye en los riesgos naturales a los que está expuesto el archivo y las particularidades del edificio ya que determina los riesgos de seguridad y las instalaciones.

Riesgos organizacionales

Los riesgos organizacionales son aquellos que provienen de la propia organización y a menudo se subestiman o ignoran. Entre ellos se encuentran:

- Falta de habilidades: El personal no tiene las habilidades o conocimientos necesarios para gestionar el archivo.
- Presupuesto insuficiente: No se asignan suficientes recursos financieros para la operación y mantenimiento del archivo.
- Procesos inadecuados: Los procesos de gestión del archivo no son eficientes o no se siguen correctamente.
- Falta de liderazgo: No hay un liderazgo claro y comprometido con la gestión del archivo digital.

Riesgos tecnológicos

Los riesgos tecnológicos se relacionan con los soportes de grabación y los formatos de representación utilizados en el archivo digital:

- Obsolescencia tecnológica de los soportes de grabación: Los soportes de almacenamiento pueden volverse obsoletos y dejar de ser compatibles con los lectores o reproductores disponibles.
- Degradación de los soportes: Los soportes de almacenamiento pueden deteriorarse con el tiempo y perder la información almacenada.
- Obsolescencia tecnológica de los formatos de representación: Los formatos de archivo pueden volverse obsoletos y dejar de ser compatibles con el software disponible.

Riesgos relacionados con el acceso

Los riesgos relacionados con el acceso se refieren a la capacidad de los usuarios para acceder a la información del archivo digital:

- Accesibilidad semántica: Los sistemas no pueden comprender el objeto de información o carecen de la información necesaria para encontrar, reconocer e identificar dicho objeto.
- Accesibilidad técnica: Los sistemas de archivo tienen dificultades para difundir los objetos de información debido a la ausencia de metadatos técnicos o una estructura inadecuada así como la presencia de sistemas de protección o cifrado de datos.
- Responsabilidades de acceso: No está claro quién tiene derecho a acceder a la información del archivo y cómo se controlan los accesos a los objetos de información de archivo

COMPLEMENTO: LA IMPLICACIÓN DE LOS LÍDERES Y LAS HABILIDADES NECESARIAS PARA EL ÉXITO DEL ARCHIVO DIGITAL

La implicación de los líderes y las habilidades necesarias para el éxito del archivo digital

El archivo digital se ha convertido en una actividad fundamental que se encuentra en la intersección entre la archivística y la tecnología de la información. El éxito de este tipo de proyectos depende en gran medida de la capacidad de los diferentes actores para trabajar en conjunto, así como de la existencia de perfiles profesionales que combinen habilidades en ambas áreas.

Dada la diversidad de competencias requeridas para la construcción del proyecto (archivística, informática, legal, calidad) y la ausencia, en la mayoría de los casos, de una estructura o servicio especializado en esta área, **es crucial que la dirección de la organización se implique de forma activa.** Esto puede hacerse mediante el nombramiento de un grupo de trabajo o la creación explícita de un proyecto dedicado al archivo digital.

Esta decisión tiene varios beneficios:

- **Visibiliza la importancia del proyecto** y demuestra el compromiso de la dirección con el mismo.
- **Permite mostrar la transversalidad del problema** a los diferentes actores internos y externos.
- **Facilita la obtención de apoyo** de los servicios y personas que se verán afectados por los cambios que implica la implementación del archivo digital.

Además de la implicación de la dirección, es necesario contar con equipos de proyecto y estructuras permanentes que estén totalmente dedicados al archivo digital. Estos equipos deben tener las diversas habilidades requeridas para el proyecto, y es importante que estas diferentes habilidades se basen en una comprensión común de los problemas a resolver.

El papel de la dirección es decisivo para el éxito del proyecto. La dirección debe mostrar su apoyo al proyecto de forma clara y visible, y debe establecer objetivos claros que sean conocidos por todas las partes interesadas.

2.4. Conclusiones sobre la gestión de riesgos

La gestión de riesgos es una herramienta fundamental para la preservación de objetos digitales. Permite utilizar los datos de los riesgos identificados para generar un panel de control que facilite la toma de decisiones y la planificación de acciones.

Este panel de control, también conocido como “plan de preservación digital”, ofrece las siguientes ventajas:

- Planificación de revisiones: Permite monitorizar la evolución de los datos, las aplicaciones y los medios de almacenamiento. Esto asegura que las opciones técnicas y organizativas elegidas sigan siendo válidas y que su calidad sea buena. Las revisiones generan informes que activan alertas en caso de detectar una situación anormal.
- Anticipación de alertas y soluciones: El sistema puede detectar problemas de forma temprana y emitir una señal de alerta. Esto permite activar un proceso de resolución de problemas predefinido, como un plan de emergencia.
- Determinación de riesgos específicos: Permite identificar los riesgos específicos de cada tipo de objeto digital y ponderar la evaluación de riesgos de acuerdo con sus particularidades técnicas o de otro tipo.

El sistema de gestión de riesgos también puede ser auditado para obtener una certificación o para priorizar acciones. La gestión de riesgos proporciona una visión general de todas las acciones de conservación que se están llevando a cabo en los objetos digitales.

En resumen, la gestión de riesgos es una herramienta esencial para la preservación digital. Permite a las organizaciones:

- Identificar y evaluar los riesgos que amenazan sus objetos digitales.
- Planificar y ejecutar acciones para mitigar estos riesgos.
- Monitorizar la eficacia de las medidas de preservación.
- Tomar decisiones informadas sobre la gestión de sus archivos digitales.

Capítulo 3. Control de costos

Cualquier proyecto de implementación de un Archivo Digital debe cumplir con los requisitos metodológicos de cualquier proyecto. Esto implica identificar las etapas y las condiciones necesarias para pasar de una etapa a la siguiente.

Antes de entrar en detalles en el análisis, es necesario establecer algunos elementos preliminares:

- La entidad de Gestión de Archivos debe estar claramente identificada. Esta entidad es la que define el mandato del Archivo y le asigna los recursos necesarios para cumplir con los objetivos derivados del mandato.
- El mandato otorgado al Archivo por la Dirección debe estar claramente explicado. Esto incluye:
    - Quiénes son los productores de información.
    - Quiénes son los usuarios del Archivo.
    - Qué servicios se les ofrecerá a los usuarios.
    - Cuáles son los objetos por archivar.
    - Cuál es el período de conservación de los objetos.
    - Cuál es el valor probatorio de los objetos.
- Los distintos aspectos regulatorios y legales deben estar explicados por escrito.
- El Archivo debe tener recursos cuantificados. Esto incluye:
    - Recursos humanos.
    - Recursos financieros.
    - Recursos tecnológicos.
- El Archivo debe tener una política de archivo. Esta política debe definir:
    - Los criterios de selección de los documentos a archivar.
    - Los procedimientos de archivo.
    - Los métodos de acceso y consulta de los documentos.
- El Archivo debe desarrollar un plan de reversibilidad. Este plan debe definir cómo se extraerán todos los datos y metadatos del Archivo en caso de que el Archivo tenga que cesar sus actividades.

Establecer estos elementos preliminares es esencial para controlar los costos del proyecto de implementación del Archivo Digital. Al tener una comprensión clara de los requisitos del proyecto, es posible realizar una planificación precisa y eficiente de los recursos necesarios.

3.1. Evaluación de costos

La evaluación de los costos del archivo digital es un ejercicio complejo, pero fundamental, tanto en el presente como en el futuro. El desarrollo exponencial de las tecnologías digitales ha generado un crecimiento exponencial en los volúmenes de datos que requieren ser archivados, a un ritmo mucho más acelerado que el de los archivos tradicionales en papel.

Es insostenible para la entidad responsable del archivo o su cliente embarcarse en una espiral de costos sin perspectivas de estabilidad o reducción. Se hace indispensable no solo estimar los costos del archivo, sino también demostrar su capacidad para operar con costos estables, incluso ante el aumento continuo de los volúmenes de información a archivar, exceptuando casos de cambios significativos en su mandato

Por ejemplo, la NASA, con su vasta experiencia en procesamiento y archivo de datos ha desarrollado una herramienta para evaluar los costos de desarrollar, operar y mantener sistemas para procesar y archivar datos científicos que se distribuye software gratuito y se encuentra disponible en el siguiente enlace: https://opensource.gsfc.nasa.gov/projects/CET/index.php

COMPLEMENTO: MODELO DE COSTO PARA LA PRESERVACIÓN DIGITAL

El Modelo de Costo para la Preservación Digital (CMDP) es una herramienta que permite a las instituciones estimar los costos asociados a la preservación digital a largo plazo. El CMDP se basa en una serie de factores, incluyendo:

- El tipo de objetos digitales a ser preservados: Esto incluye formatos de archivo, tamaño y complejidad.
- Las estrategias de preservación a ser utilizadas: Esto incluye la replicación, la migración y la emulación.
- La infraestructura de TI utilizada: Esto incluye hardware, software y almacenamiento.
- Los recursos humanos necesarios: Esto incluye personal con las habilidades y conocimientos necesarios para la preservación digital.

El CMDP se puede utilizar para:

- Planificar y presupuestar proyectos de preservación digital.
- Comparar los costos de diferentes estrategias de preservación.
- Justificar la inversión en preservación digital a las partes interesadas.

Puede consultarse información adicional de este modelo en los siguientes enlaces:

- https://www.4cproject.eu/summary-of-cost-models/16-community-resources/outputs-and-deliverables/108-cost-model-for-digital-preservation-cmdp/
- https://coptr.digipres.org/index.php/CMDP_(Cost_Model_for_Digital_Preservation)

3.2. El estudio realizado para los servicios públicos de archivo

En un estudio de costos, es fundamental analizar el impacto del modelo organizativo seleccionado, especialmente en lo que respecta a la puesta en común de recursos.

Esta influencia se ha demostrado en estudios realizados, por ejemplo, en el ámbito de los servicios públicos de archivo.

De esta forma, puede citarse un estudio sobre el desarrollo de plataformas de archivo electrónico para servicios públicos de archivo, realizado por Parker Williborg a petición de la Dirección de Archivos de Francia, donde se aborda la cuestión de la evaluación de costos en la esfera pública.

En particular, analiza el impacto del modelo organizativo elegido y, por tanto, el impacto de la puesta en común de los recursos en los costes. Se estudiaron cinco escenarios, desde una plataforma local y aislada hasta una plataforma nacional y compartida en gran parte:

- Escenario 1: una plataforma dedicada a un único servicio de productor que almacena su propio archivo o tiene un servicio de archivo interno (por ejemplo, un gran municipio, un consejo general)
- Escenario 2: una plataforma dedicada a un conjunto de servicios locales de productores (como servicios de archivo departamentales o algunos servicios de archivos municipales importantes).
- Escenario 3: una plataforma nacional dedicada a todos los servicios centrales y descentralizados en el marco del mismo ministerio.
- Escenario 4: una plataforma nacional dedicada a un conjunto de comunidades del mismo tipo (consejos generales, consejos regionales)
- Escenario 5: una plataforma nacional para todas las administraciones del gobierno central (Archivos Nacionales)

EJEMPLO: APLICACIÓN DEL ESTUDIO

Estimación de volúmenes para los próximos 10 años

La estimación de volúmenes para los próximos 10 años se basa en la identificación de fuentes candidatas para el archivo electrónico. Se ha considerado la retención de todos los datos duplicados para garantizar la integridad de la información archivada.

Estimación de recursos humanos

La estimación de recursos humanos necesarios se fundamentó en un análisis detallado de las funcionalidades de la plataforma, desglosadas por proceso principal (preparación y soporte de pagos, almacenamiento, gestión de datos descriptivos, restitución) y por funciones transversales (administración de la plataforma, pilotaje, seguimiento tecnológico y legal, desarrollo y proyectos de migración).

A continuación, se desglosaron las tareas con la determinación de un tiempo medio por tarea y un costo horario de los agentes. Se elaboraron distintas estimaciones en función de la elección de mayor o menor automatización de los procesos, el uso de redes o medios extraíbles para transmisiones, la instalación de plataformas manuales (soportes en estanterías) o automatizadas, etc.

Evaluación de costos iniciales y costos anuales

El funcionamiento de la plataforma de archivo electrónico se basó en el supuesto de desarrollo a nivel nacional utilizando paquetes de software de mercado (que requerirían un trabajo de integración significativo) y una solución genérica siguiendo estos pasos:

1. Desarrollo
2. Despliegue piloto
3. Generalización de la solución

Este enfoque condujo al desarrollo de la plataforma piloto Pilze.

Partiendo de la disponibilidad de la plataforma genérica, se estimaron los costos específicos de cada plataforma implementada. Estos costos incluyen, por un lado, los costos iniciales de adquisición de la plataforma operativa, instalación de la solución genérica adecuada y costos internos de puesta en marcha con los departamentos productores. Por otro lado, se consideraron los costos operativos anuales, que varían según el proceso (pago de licencias, costo de gestión de almacenamiento, costo de devoluciones y consultas, costo de aplicación y mantenimiento técnico, costo de funciones transversales).

Análisis de escenarios y comparación de costos por terabyte

Se realizaron análisis de escenarios y comparaciones de costos por terabyte. Los resultados revelan que, a medida que aumentan los volúmenes archivados, las economías de escala son considerables:

- Los costos por terabyte son consistentemente superiores a veinte veces entre el primer escenario (plataforma de archivo dedicada a un único servicio productor) y el último (plataforma nacional), tanto para costos externos iniciales como operativos. Por lo tanto, se recomienda fomentar el uso de plataformas de mayor tamaño.
- Los costos internos más significativos están relacionados con el inicio de un proceso de archivo con un nuevo servicio de productor (nuevo productor/nueva aplicación). Estos costos son particularmente elevados para las categorías A al inicio y las categorías B para la operación. Esto aplica tanto al servicio de archivo como al productor, quien deberá adaptar su aplicación para la transferencia al formato definido por el esquema de transferencia XML a la plataforma de archivo.

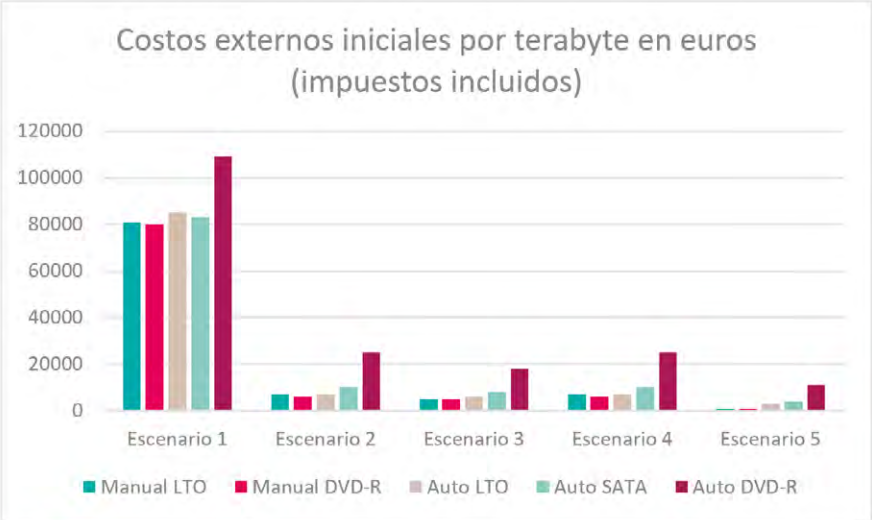
Recomendaciones

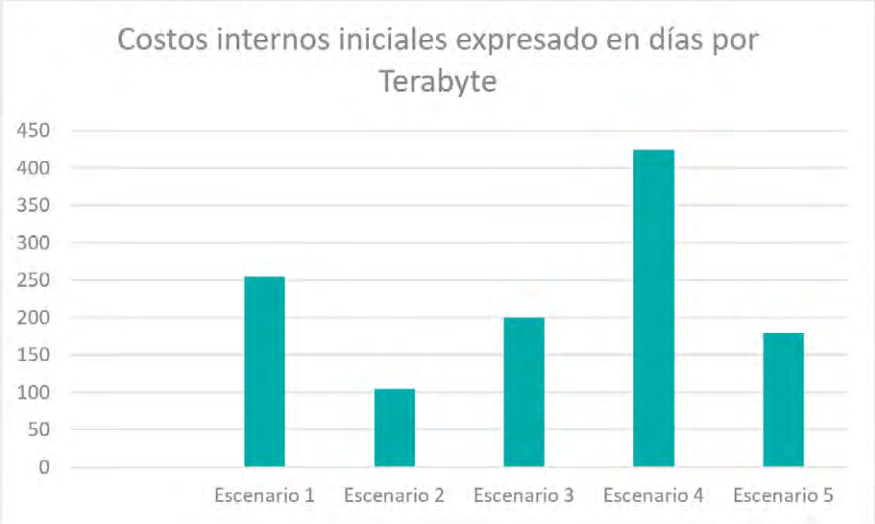
En base a los resultados del estudio, se recomienda:

- Priorizar los pagos de gran volumen para optimizar los costos.
- Limitar el número de diferentes servicios de producción, si no se dispone de suficientes recursos humanos.

- Fortalecer el nivel central (Dirección de Archivos de Francia) para proporcionar asistencia en el modelado de pagos por categorías principales de documentos, que se encuentran en todos los sitios (ejemplo: mercados públicos).

De esta forma, el gráfico a continuación expresa los costos iniciales en función de los escenarios enumerados anteriormente con la implementación de diferentes tipos de almacenamiento:





Caso de un único servicio productor que garantiza su propio archivo

	PLATAFORMA MANUAL /LTO		
	Costos externos (euros con IVA)	**Costo por día del servicio para un Agente categoría A**	**Costo por día del servicio para un Agente categoría B**
Costos iniciales			
Adquisición de la plataforma Explotación	39 468,00		
Instalación y desarrollo en el sitio	42 338,40	50	
Inicio de los servicios productores		10	
Inicio de las aplicaciones fuente		200	
Total	**81 806,40**	**260**	**0**
Costo por Terabyte	**81 806,40**	**260**	**0**
Costo de explotación anual			
Pagos			27,58
Almacenamiento	388,7		0,20
Consulta/restitución	299		10,15
mantenimiento de las aplicaciones	8 467,68	10	
Explotación y mantenimiento técnico	10 405,20		40
Funciones transversales[1]		35	95
Cargos variables de administración[2]		21,8	
Total	**19 560,58**	**66,8**	**172,96**
Costo por Terabyte	**19 560,58**	**66,8**	**172,96**

Caso de una plataforma nacional para todos los organismos del gobierno central

	PLATAFORMA AUTOMATIZADA /LTO		
	Costos externos (euros con IVA)	**Costo por día del servicio para un Agente categoría A**	**Costo por día del servicio para un Agente categoría B**
Costos iniciales			
Adquisición de la plataforma Explotación	222 755,00		
Instalación y desarrollo en el sitio	42 338,40	50	

1 Excluidos los costos variables de Administración.

2 igual al 10% de la plantilla (agentes categoría A y B)

	PLATAFORMA AUTOMATIZADA /LTO		
	Costos externos (euros con IVA)	**Costo por día del servicio para un Agente categoría A**	**Costo por día del servicio para un Agente categoría B**
Inicio de los servicios productores		200	
Inicio de las aplicaciones fuente		1600	
Total	**265 093,40**	**1850**	**0**
Costo por Terabyte	**2 650,93**	**18,5**	**0**
Costo de explotación anual			
Pagos			220,6
Almacenamiento	38870		
Consulta/restitución	5980		78
mantenimiento de las aplicaciones	8 467,68	10	
Explotación y mantenimiento técnico	47 062,60		40
Funciones transversales[3]		35	190
Cargos variables de administración[4]		57,36	
Total	**100 380,28**	**102,36**	**528,6**
Costo por Terabyte	**1 003,80**	**1,02**	**5,29**

3.3. Factores a tener en cuenta en el cálculo de costes

Cuadro resumen de los factores de costo a tener en cuenta.

Aspectos a tener en cuenta	**Recursos humanos**		**Infraestructura: hardware, locales, redes**		**Validación y desarrollo de software**	
	Implementación	Operación	Implementación	Operación	Implementación	Operación
Cantidad de servicios productores (número de protocolos de pago, número de contactos)	Alto	Alto				

3 Excluidos los costos variables de Administración.

4 igual al 10% de la plantilla (agentes categoría A y B)

Aspectos a tener en cuenta	**Recursos humanos**		**Infraestructura: hardware, locales, redes**		**Validación y desarrollo de software**	
	Implementación	Operación	Implementación	Operación	Implementación	Operación
Naturaleza de las relaciones con los productores: ¿es posible imponer formatos de archivo o el Archivo se verá obligado a migrar formatos desde el principio, suministro completo de metadatos o no?	Alto				Alto	
Complejidad del contenido (Asociación de elementos documentales con objetos de información archivados)	Alto	Alto				
Número y complejidad de los formatos de datos.	Alto				Alto	Alto
Proporción de documentos sujetos a limitaciones de valor probatorio (que implican el uso sistemático de firmas electrónicas, cálculos de huellas dactilares y sellado de tiempo)	Alto		Alto		Alto	
Bajo nivel de automatización de pagos (posible existencia de operaciones manuales sistemáticas)		Alto				
Alto nivel de automatización de pagos					Alto	Alto
Disponibilidad de componentes de software reutilizables					Alto	
Alto volumen (impacto en la capacidad de los recursos de almacenamiento, en el monitoreo de las operaciones y su renovación periódica como parte de las migraciones de soporte)		Mediano	Alto	Alto		
Granularidad de los objetos (la gestión de un gran número de objetos no deja de tener consecuencias sobre las limitaciones que pesan sobre la base de datos)			Alto		Mediano	
Requisitos de seguridad, criticidad y confidencialidad de los datos	Alto		Alto		Alto	

Aspectos a tener en cuenta	**Recursos humanos**		**Infraestructura: hardware, locales, redes**		**Validación y desarrollo de software**	
	Implementación	Operación	Implementación	Operación	Implementación	Operación
Requisitos de continuidad del servicio: tasas de indisponibilidad aceptables. Un servicio abierto las 24 horas del día con un bajo índice de indisponibilidad debe contar con recursos redundantes y un sistema de guardia		Alto	Alto	Alto	Mediano	Mediano
Número de usuarios que pueden consultar el servicio en paralelo			Alto			
Requisitos de nivel de servicio para que los usuarios accedan a los documentos de forma más o menos rápida, interfaz y medios sofisticados de búsqueda y recuperación.			Alto		Alto	
Atención al cliente (gestión de usuarios y sus derechos de acceso)		Alto				Mediano a Alto
Frecuencia de auditorías de paquetes pagos y paquetes archivados		Alto				
Soporte gratuito para los usuarios (si el soporte es de pago, éste constituirá una fuente de recursos para el Archivo)		Alto				
Seguimiento tecnológico, seguimiento de la evolución de las normas, necesidades de los usuarios, etc.		Alto				

3.4. Formas de reducir costos

Las primeras vías para examinar son internas del Archivo y se enfocan en su organización, funcionamiento, equipamiento y racionalización de sus actividades.

En cuanto a la reducción de costos, las posibilidades de compartir gastos con otros Archivos u otros departamentos de la organización son diversas y numerosas. El objetivo principal es distribuir los costos de la manera más amplia posible, considerando las siguientes estrategias:

1. Reutilización de la infraestructura de TI existente en la organización:

- Aprovechar los recursos informáticos ya disponibles dentro de la organización para reducir la necesidad de inversiones adicionales.

2. Compartir infraestructura de almacenamiento:

- La experiencia demuestra que configurar y administrar una infraestructura de almacenamiento requiere habilidades y recursos humanos similares, independientemente de la cantidad de datos almacenados (50 TB o 500 TB).
- Explorar acuerdos de reciprocidad con otros Archivos para compartir infraestructura de almacenamiento, garantizando la seguridad y redundancia de los datos digitales en dos sitios separados geográficamente distantes.

3. Desarrollo de sistemas de software genéricos adaptables a múltiples contextos:

- Implementar un enfoque modular en el desarrollo de software, permitiendo la reutilización de componentes y la adaptación a diferentes necesidades dentro del mismo dominio.
- Un ejemplo de este enfoque es un servicio de archivos que recibe archivos de varios productores pero utiliza una única herramienta de búsqueda para todos los fondos archivados, independientemente de los campos administrativos.

4. Reutilización de componentes de software de la aplicación de archivo:

Fomentar la reutilización de componentes de software gratuitos o comerciales para reducir costos de desarrollo y optimizar recursos.

En un campo específico, como el de los servicios de archivos públicos, archivos científicos u otros, el 90% de las necesidades de software pueden ser comunes.

Diseñar software considerando la reutilización para generar interés en las empresas de software y optimizar costos para los Archivos.

En el área de pago, se deben considerar dos puntos importantes:

1. Límites de pago vinculadas al archivo de documentos:

- Considerar las limitaciones de pago en el momento de la creación del documento o cuando el documento se bloquea y deja de ser modificable.
- Implementar mecanismos para gestionar pagos de manera eficiente y segura.

2. Máxima automatización del proceso de transferencia y creación de paquetes de información archivados:

- Automatizar el proceso de transferencia de archivos, asegurando la estandarización de los paquetes SIP (Standard Information Package).
- Automatizar la creación de paquetes de información archivados para optimizar el almacenamiento y la gestión de datos.

El trabajo de definición de estándares no debería ser responsabilidad de un solo Archivo.

- Es recomendable reutilizar los estándares existentes y compartir la tarea de redacción de nuevos estándares con otros Archivos cuando surjan nuevas necesidades.
- La colaboración entre Archivos permitirá establecer estándares eficientes y adecuados para la gestión de archivos digitales.

EJEMPLO

La Dirección de Archivos de Francia y la Dirección General de Modernización del Estado ponen a disposición de todos los servicios de archivos públicos modelos de descripción, no componentes de software. Estos modelos cumplen con el estándar de "intercambio de datos para el archivo" y son esenciales para desarrollar transferencias. Los modelos están disponibles para una categoría de archivos que se pueden encontrar en todo el territorio nacional.

Capítulo 4. Desarrollo de una política de archivo

Con la tecnología digital, los riesgos de litigio se vuelven más importantes: determinación de los roles y responsabilidades de los diversos actores que intervienen a lo largo del ciclo de vida del documento, problemas de integridad (¿cómo probar que el documento original no ha sido modificado?), Problemas de conversión de formato. (cómo demostrar que el documento convertido no ha perdido la funcionalidad original), problemas de medios defectuosos que han dañado o hecho desaparecer los datos, problemas de derechos de acceso, por ello es necesario especificar, en el marco de una política de archivo, todos los elementos que participarán en la implementación del proceso de archivo adecuado para asegurar que un documento ha sido adecuadamente integrado, controlado, conservado, gestionado y consultado a lo largo de su ciclo de vida.

4.1. Objetivos de la política o carta de archivo

La acción del archivista será tanto más eficaz cuando exista una carta de archivo dentro de la organización, validada al más alto nivel y válida para toda la información recibida o producida en la organización, cualquiera que sea su forma. Por tanto, la carta o política de archivo debe aplicarse a toda la producción con especificidades obviamente vinculadas a la producción digital.

La carta o política de archivo establecerá las buenas prácticas que sustentan la gestión archivística. Definirá el marco legal vigente, identificará a los actores involucrados y detallará sus respectivas obligaciones y responsabilidades. En este sentido, la política de archivo establece los requisitos mínimos, en términos legales, funcionales, operativos, técnicos y de seguridad, que debe cumplir un archivo electrónico para ser considerado confiable. Estos requisitos se basan en las restricciones "estándar" que deben implementarse y que se enumeran a continuación:

Restricciones materiales

- Identificación y autenticación del origen de los documentos archivados.
- Integridad de los archivos.
- Inteligibilidad y legibilidad de los archivos.
- Vida útil de los archivos.
- Trazabilidad de las diversas operaciones (creación, modificación, consulta, eliminación).
- Disponibilidad y accesibilidad de los archivos

Esta carta o política constituye un marco de referencia fundamental para garantizar la confiabilidad de un archivo electrónico. Una matriz de auditoría compuesta por sus diferentes capítulos permite al auditor evaluar la confiabilidad de un servicio de archivo electrónico. La auditoría debe verificar, en particular, que se hayan definido los procesos para aplicar la política de archivo y que estos procesos se apliquen efectivamente. La persona responsable de la implementación de la política de archivo debe estar claramente designada y ser conocida por las partes interesadas, quienes pueden requerir su asistencia con fines informativos y operativos.

La carta de archivo es un documento de alto nivel que debe complementarse con documentos más detallados que describan su implementación en términos de organización, procesos y procedimientos.

4.2. Responsabilidades y obligaciones de las distintas partes

La autoridad de archivo es la entidad responsable del archivo (gestión, tratamiento, conservación y comunicación de los datos).

De hecho, a lo largo del ciclo de vida de un documento, puede haber varias autoridades de archivo sucesivas: en el sector público, el servicio de productor mientras el archivo esté “vivo”, luego un servicio de archivo intermedio para la “edad intermedia” y finalmente un servicio de archivo definitivo para la “edad definitiva”; o el productor durante las edades vivas e intermedias, y el servicio de archivo para la edad final. La transferencia anticipada de datos al servicio de archivo antes de que finalice el período intermedio no modifica esta distribución de responsabilidades.

Por su parte, el departamento de TI tendrá un rol de operador que ejercerá inicialmente para el departamento de producción y, en segundo lugar, para el departamento de archivos cuando este último se convierta en la Autoridad de Archivo.

El contrato o acuerdo así celebrado entre los diferentes actores del proceso (departamento de producción, departamento de archivos, departamento de TI) define el alcance de los datos a transferir / eliminar así como los procesos de transferencia y eliminación.

El análisis general de las interfaces e interacciones entre el servicio de depósito y el servicio de archivo electrónico es el tema de la norma ISO20652: 2006 “Estándar abstracto de metodología de interfaz de archivo de productor”. Este estándar se estudia en la parte 5 sobre el modelo OAIS y los estándares derivados y puede estudiarse a detalle en la norma ISO14721 “Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia”.

Finalmente, los demás actores del proceso (administradores, usuarios) tendrán un cierto número de obligaciones y responsabilidades a definir en el marco de esta política de archivo, en particular en términos de acceso a la información.

4.3. Obligaciones del servicio productor

El servicio productor debe garantizar lo siguiente:

- Gestión del sistema de información:
    - Alimentar y actualizar el sistema de información.
    - Informar al departamento de informática sobre duplicados, errores y archivos vacíos.
- Integración del ciclo de vida de los datos digitales:
    - Integrar el ciclo de vida de los datos digitales en el sistema de información.
- Transferencia de archivos cerrados:
    - Si existe un módulo de archivo interno o una base de datos de archivo intermedia, transferir los archivos cerrados y generar un informe de esta base de datos en caso de datos personales.
    - Mantener la integridad de los datos en esta base de datos.
- Aspectos volumétricos y calendario de traslados:
    - Proporcionar información sobre los aspectos volumétricos de los traslados al servicio de archivos.
    - En su caso, proporcionar un calendario provisional de futuros traslados.
- Medios y protocolos de transferencia:
    - Definir los medios que se pueden utilizar para las transferencias que no utilicen una red informática.
    - Para las transmisiones en red, definir los protocolos que se utilizarán.
- Formatos de codificación de datos:
    - Definir los formatos de codificación de datos que acepta el servicio de archivos.
    - Si el formato original de los archivos no permite garantizar una buena continuidad de la información, definir los métodos de conversión de formatos que el servicio de archivos desea realizar a la llegada de los archivos transferidos.
- Información sobre los archivos transferidos:
    - Proporcionar toda la información relativa a la naturaleza y duración de los archivos transferidos, así como su posible confidencialidad y acceso limitado.
    - El departamento de productores es responsable de la veracidad de esta información y su correcta transmisión.
- Cumplimiento de los requisitos técnicos:
    - Cumplir con los requisitos técnicos definidos por la Autoridad de Archivo.

    - En particular, cumplir con un formato de intercambio de datos y garantizar que los medios y los archivos que contienen se encuentren en perfecto estado y libres de virus u otras anomalías que puedan tener un impacto en la correcta ejecución de la política de archivo.
- Verificación de firmas digitales:
    - En el caso de documentos firmados digitalmente que se vayan a transferir al servicio de archivos, verificar su firma antes de la transferencia prevista.
    - Ingresar los resultados de esta verificación en los metadatos de los documentos en cuestión.

Durante la transferencia, la generación de huellas dactilares de los archivos transferidos con el fin de permitir a la Autoridad de Archivo verificar la integridad de este último cuando sea recibido.

4.4. Obligaciones del departamento de Tecnologías de la Información

En su calidad de operador de archivo, las unidades de TI deben comprometerse a lo siguiente:

- Ejecutar las operaciones de transferencia o eliminación de datos digitales en nombre de la Autoridad de Archivo.
- Garantizar la eliminación física de los datos digitales una vez finalizado su período de utilidad administrativa, previa obtención del visto bueno para la eliminación por parte del servicio de archivos.
- Emitir un informe detallado sobre la destrucción de los datos eliminados.
- Garantizar un acceso seguro a los usuarios del Archivo mediante la implementación de una gestión de autorizaciones adecuada y la provisión de medios de acceso dimensionados de acuerdo con las necesidades y los recursos disponibles.
- Asegurar el desarrollo e implementación de los cambios necesarios.
- Administrar y operar los sistemas de manera eficiente y eficaz.
- Garantizar la fiabilidad operativa de los sistemas mediante el establecimiento de un plan de recuperación o continuidad del negocio acorde al nivel de calidad de servicio requerido por los usuarios.
- Proteger la integridad de los objetos digitales a través de un almacenamiento seguro de datos digitales que incluya redundancia, replicación en varios sitios remotos, monitoreo constante de los medios y migración periódica de dichos medios.
- Mantenerse a la vanguardia de la evolución tecnológica de la infraestructura.
- Implementar las operaciones de migración solicitadas por el servicio de archivos, incluyendo prototipado, pruebas exhaustivas y seguimiento de la ejecución.

4.5. Obligaciones del servicio de archivo

El servicio de archivo se encarga de:

- Definir, en colaboración con el departamento de producción, las reglas relativas al ciclo de vida de los datos en el sistema de información.
- Examinar las solicitudes de visado de eliminación que se le dirigen.

- Recibir, en el formato de intercambio especificado, los archivos transferidos y verificarlos para su validación o rechazo. Si el control resulta satisfactorio, generar un mensaje de aceptación de la transferencia que, potencialmente, pueda estar cubierto por una firma digital. Este mensaje debe indicar la asunción de responsabilidad y, por lo tanto, la responsabilidad de la Autoridad de Archivo por los archivos transferidos.
- Aplicar, en caso de transferencia antes de la expiración del período de utilidad administrativa (DUA), el período de conservación adecuado para los archivos en cuestión de acuerdo con las instrucciones dadas por el departamento de producción.
- Definir las reglas que permiten el almacenamiento de datos a largo plazo, que debe implementar el departamento de TI.
- Verificar todos los accesos al servicio de archivos, tanto físicos como lógicos, internos y externos, de acuerdo con los derechos de cada una de las partes involucradas.
- Permitir el acceso a los archivos procesados solo a las personas autorizadas.
- Solicitar al servicio de productores su autorización para cualquier solicitud de comunicación de los archivos en cuestión, siempre que no hayan expirado los plazos de libre comunicación.
- Exigir la firma de un acuerdo de secreto y confidencialidad por parte de todo el personal externo y por los subcontratistas.
- Tomar una serie de medidas tan pronto como transfiere los archivos que es responsable de preservar a otra autoridad de archivo (por ejemplo, de un servicio de archivos intermedio a un servicio de archivos definitivo).

COMPLEMENTO

Ejemplos de políticas de archivo

Sobre el desarrollo de políticas de archivo puede consultarse el modelo desarrollado por el gobierno de España, disponible en el siguiente enlace: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Archivo_electronico/pae_Politica-de-gestion-de-documentos-electronicos.html

Asimismo, puede consultarse la Guía de Implementación Gerencial– Política de gestión de documentos y archivos que forma parte del Modelo de Gestión de Documentos y Administración de Archivos (MGD) para la Red de Transparencia y Acceso a la Información (RTA) y que se encuentra disponible en el siguiente enlace: http://mgd.redrta.org/guia-de-implementacion-gerencial-politica-de-gestion-de-documentos-y-archivos/mgd/2015-01-21/124946.html

Modelos de requisitos

Por otra parte, puede consultarse el modelo propuesto el modelo MoReq2010, disponible en el siguiente enlace: https://moreq.info/

Además, sobre los estándares y aplicaciones basadas en el modelo de referencia OAIS se recomienda profundizar en los trabajos desarrollados por el proyecto E-ARK y mantenidas por la Digital Information LifeCycle Interoperability Standards Board (DILCIS Board), toda la información relacionada con esta iniciativa está disponible en el siguiente enlace: https://dilcis.eu/

Capítulo 5. Política de seguridad a implementar

La gestión de archivos digitales implica la captura, almacenamiento, conservación, acceso y eliminación de datos electrónicos. La seguridad de los archivos digitales es fundamental para garantizar la confidencialidad, integridad y disponibilidad de la información, así como para cumplir con las regulaciones legales y normativas aplicables.

En este contexto, la Autoridad de Archivo debe establecer e implementar una Política de Seguridad de Sistemas de Información (PSSI) alineada con los estándares y regulaciones aplicables a la organización o institución a la que pertenece. Esta política de seguridad debe abordar los aspectos específicos de la gestión de archivos y garantizar la protección adecuada de los datos y sistemas archivísticos.

Asimismo, la Autoridad de Archivo mantiene la responsabilidad general por la seguridad de todos los procesos de archivo, incluso si ciertas funciones de estos procesos se delegan a componentes externos. Es responsabilidad de la Autoridad de Archivo:

- Establecer e implementar una PSSI integral que abarque todos los aspectos de la gestión de archivos. Esto incluye la definición de roles y responsabilidades en materia de seguridad, la identificación y evaluación de riesgos, la implementación de medidas de seguridad técnicas y no técnicas, la gestión de incidentes de seguridad y la realización de auditorías periódicas.
- Garantizar el cumplimiento de los requisitos de seguridad establecidos en la PSSI por parte de todos los componentes internos y externos involucrados en los procesos de archivo. Esto puede requerir la negociación de acuerdos de seguridad con proveedores externos y la implementación de mecanismos de control para garantizar el cumplimiento de los requisitos de seguridad.
- Implementar mecanismos de monitoreo y control para garantizar la aplicación efectiva de la PSSI. Esto puede incluir la instalación de herramientas de monitoreo de seguridad, la realización de pruebas de penetración y la realización de auditorías internas de seguridad.
- Fomentar la participación de la dirección de la Autoridad de Archivo en la definición e implementación de la política de seguridad de la información. El compromiso de la dirección es esencial para garantizar la asignación de recursos adecuados y la creación de una cultura de seguridad dentro de la organización.
- Realizar análisis de riesgos periódicos para identificar y evaluar los riesgos potenciales que puedan afectar la seguridad de los archivos y sistemas archivísticos. El análisis de riesgos debe considerar amenazas internas y externas, así como las vulnerabilidades de los sistemas y procesos de archivo.
- Definir objetivos de seguridad específicos y medibles para mitigar los riesgos identificados en el análisis de riesgos. Los objetivos de seguridad deben ser realistas, alcanzables y alineados con las estrategias de seguridad de la organización.
- Implementar medidas de seguridad técnicas y no técnicas adecuadas para cumplir con los objetivos de seguridad establecidos. Las medidas de seguridad técnicas pueden incluir firewalls, sistemas de detección de intrusiones, software antivirus y antimalware, encriptación de datos y mecanismos de copia de seguridad. Las medidas de seguridad no técnicas pueden incluir capacitación en seguridad para el personal, procedimientos de seguridad documentados, gestión de riesgos y vulnerabilidades, auditorías de seguridad y monitoreo continuo de sistemas y redes.

- Establecer un nivel mínimo de garantía de seguridad para los sistemas de TI de la Autoridad de Archivo. Este nivel mínimo debe considerar los aspectos de confidencialidad, integridad, disponibilidad, no repudio y autenticidad de la información archivística.
- Documentar la PSSI y mantenerla actualizada de manera regular. La PSSI debe ser un documento claro, conciso y fácil de entender que esté disponible para todas las partes interesadas. La PSSI debe revisarse y actualizarse periódicamente para reflejar los cambios en el entorno de seguridad y las necesidades de la organización.
- Análisis de riesgos y objetivos de seguridad. La Autoridad de Archivo debe realizar un análisis de riesgos periódico para identificar y evaluar los riesgos potenciales que puedan afectar la seguridad de los archivos y sistemas archivísticos. Este análisis debe considerar todos los aspectos de los procesos de archivo, desde la creación y captura de datos hasta la conservación y eliminación de archivos.
- Al realizar el análisis de riesgos, la Autoridad de Archivo debe considerar los siguientes factores:
- Amenazas: Las amenazas pueden ser internas o externas. Las amenazas internas pueden incluir errores humanos, sabotaje y robo de datos. Las amenazas externas pueden incluir ataques cibernéticos, desastres naturales y fallas de energía.
- Vulnerabilidades: Las vulnerabilidades son debilidades en los sistemas o procesos que pueden ser explotadas por las amenazas. Las vulnerabilidades pueden ser técnicas o no técnicas. Las vulnerabilidades técnicas pueden incluir errores de software, configuraciones incorrectas y hardware vulnerable. Las vulnerabilidades no técnicas pueden incluir falta de capacitación del personal, procedimientos de seguridad inadecuados y controles de usuarios.

COMPLEMENTO

Puede consultar el sitio de la Agencia Nacional para la Seguridad de los Sistemas de Información del gobierno francés, para comprender laaplicación de políticas de seguridad, disponible en el siguiente enlace: https://cyber.gouv.fr/ , asimismo, puede consultar el Esquema Nacional de Seguridad, desarrollado por el Gobierno de España y disponible en el siguiente enlace: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html

5.1. Roles de confianza

En cuanto a las responsabilidades del nivel operativo, debemos distinguir al menos los siguientes roles funcionales de confianza:

1. Gerente de seguridad:

- Responsable de implementar y asegurar la aplicación de la política de seguridad.
- Gestiona los controles de acceso físico al equipo.
- Autorizado para conocer los archivos relacionados con la actividad de la Autoridad de Archivo.
- Analiza los registros de eventos para detectar incidencias, anomalías e intentos de compromiso.

2. Administrador de la aplicación:

- Responsable de implementar la política de archivo en el nivel de la aplicación a su cargo.
- Supervisa todas las funciones y el desempeño de la aplicación.

3. Ingeniero de sistemas:

- Responsable de la puesta en marcha, configuración y mantenimiento técnico de los equipos informáticos.
- Asegura la administración técnica de sistemas y redes.

4. Administrador funcional:

- Gestiona los perfiles de usuarios para una aplicación determinada.

5. Administrador de base de datos:

- Administra las bases de datos en las que se basan las aplicaciones, con especial atención a los derechos de acceso.

6. Agente de servicio de archivo electrónico:

- Explota las aplicaciones dentro del marco de sus atribuciones.

Combinaciones de roles prohibidas:

- Gerente de seguridad e ingeniero de sistemas
- Operador evaluador y cualquier otro rol
- Ingeniero de sistemas y operador

5.2. Identificación, autenticación, integridad

Control de acceso y autenticación de usuarios

Una vez que un usuario ha sido identificado y autenticado, es fundamental establecer un sistema de control de acceso que limite su acceso a los recursos y datos en función de sus derechos y permisos. Este sistema debe basarse en un directorio centralizado que almacene información actualizada sobre todos los usuarios y sus respectivos derechos. El directorio debe actualizarse periódicamente para reflejar cualquier cambio en los permisos o roles de los usuarios.

Para garantizar la seguridad y confiabilidad del acceso a los sistemas de archivo, es esencial implementar mecanismos de autenticación robustos que permitan verificar con precisión la identidad de los usuarios. Si bien una contraseña simple puede ser suficiente para consultas básicas del sistema, para accesos más sensibles, como aquellos relacionados con la administración, se deben emplear métodos de autenticación más fuertes, como el uso de certificados electrónicos.

Control de acceso a archivos confidenciales

En el caso de archivos confidenciales, el control de acceso debe ser gestionado exclusivamente por el servicio de archivo electrónico, restringiendo el acceso únicamente a las personas autorizadas. El servicio de archivo debe implementar mecanismos que permitan auditar y rastrear el acceso a estos archivos sensibles.

Verificación de integridad de archivos custodiados

La verificación de la integridad de los archivos custodiados debe realizarse en múltiples etapas del proceso de archivo:

- Nivel de transferencia: El servicio de archivos debe verificar la integridad de los archivos durante la transferencia inicial para garantizar que no hayan sido alterados durante el proceso de transmisión.
- Ciclo de vida del archivo: La verificación de integridad debe ser posible en cualquier momento durante el ciclo de vida del archivo, independientemente de posibles migraciones o consultas por parte de los usuarios. Para archivos físicos, se pueden realizar verificaciones periódicas mediante muestreo a través de la impresión de documentos y la comparación con copias de referencia.

Implementación de sistemas de verificación de integridad

La selección y aplicación de sistemas de verificación de integridad debe considerar los siguientes aspectos:

- Tipo de archivo: Los métodos de verificación deben adaptarse al tipo de archivo (físico, digital, etc.) y a las características específicas del formato.
- Nivel de riesgo: El nivel de riesgo asociado al archivo debe determinar la frecuencia y el rigor de las verificaciones de integridad.
- Recursos disponibles: La implementación de sistemas de verificación debe considerar los recursos técnicos y humanos disponibles.

5.3. Trazabilidad

Para conformar un conjunto de datos suficiente y coherente en términos de trazabilidad, es necesario realizar y validar las siguientes operaciones antes de poner en marcha cualquier servicio de archivo electrónico:

1. Identificación de eventos a registrar

El primer paso consiste en identificar los diferentes tipos de eventos que se registrarán en el sistema de archivo electrónico. Esto incluye eventos relacionados con la creación, modificación, eliminación, acceso y transferencia de archivos, así como eventos relacionados con la configuración y el mantenimiento del sistema.

2. Definición de información registrada

Para cada tipo de evento identificado, se debe definir la información que se registrará. Esta información debe ser suficiente para permitir la trazabilidad completa de las acciones realizadas dentro del sistema.

3. Notificaciones de eventos

Se debe determinar si se debe notificar al administrador de eventos la grabación de un evento, y en qué términos. Esto dependerá del tipo de evento y de su potencial impacto en la seguridad o el funcionamiento del sistema.

4. Frecuencia de procesamiento de registros

Se debe definir una frecuencia mínima de procesamiento de los registros de eventos. Esto asegurará que los registros se procesen de manera oportuna y que la información esté disponible para su análisis en caso de necesidad.

5. Retención de registros

Se debe establecer un período de retención para los registros de eventos. Este período debe ser lo suficientemente largo para permitir la investigación de incidentes de seguridad o problemas de funcionamiento, pero no debe ser excesivo para evitar la acumulación de datos innecesarios.

6. Seguridad de los registros

Se deben verificar los dispositivos de seguridad implementados para proteger los registros de eventos. Esto incluye medidas de control de acceso, protección contra intrusiones y copias de seguridad.

7. Procedimiento de almacenamiento de registros

Se debe consultar el procedimiento establecido para el almacenamiento de los registros de eventos. Esto asegurará que los registros se almacenen de manera segura y que sean accesibles para su consulta y análisis.

8. Sello de tiempo

Con el fin de garantizar la integridad del sello de tiempo realizado por el servicio, este último se basará en un proceso acorde con el estado del arte. Actualmente, el RFC 3161 proporciona una referencia para la implementación de sellos de tiempo confiables. Además, se recomienda utilizar al menos dos fuentes de tiempo separadas para fechar las diferentes operaciones realizadas. Esto ayudará a prevenir la manipulación del sello de tiempo y a garantizar la confiabilidad de los registros de eventos.

5.4. Plan de continuidad del negocio

Cada componente de la Autoridad de archivo debe tener un plan de continuidad comercial para cumplir con los requisitos de disponibilidad de las diversas funciones del proceso de archivo que debe ser sometió a prueba al menos anualmente.

Por lo tanto, cada entidad que opera un componente de la Autoridad de Archivos debe implementar procedimientos y medios para informar y manejar incidentes, en particular mediante la sensibilización y capacitación de su personal y mediante el análisis de los diversos registros de eventos.

Capítulo 6. Conclusión

La incorporación del enfoque de sostenibilidad en el ámbito archivístico no se limita a la mera implementación de un nuevo sistema, sino que exige una profunda reestructuración y reorientación de la organización desde una perspectiva holística. Este enfoque implica una transformación multifacética que abarca diversos aspectos, desde los presupuestarios y organizativos hasta los profesionales, técnicos y culturales.

Si bien no se trata de una revolución radical, sino de una evolución gradual, el proceso de adopción de la sostenibilidad puede presentar desafíos considerables, especialmente en función del grado de madurez de la organización. Sin embargo, es importante destacar que no se parte de cero, ya que existen prácticas y metodologías reconocidas que pueden adaptarse al contexto archivístico. Los fundamentos del archivo, la gestión de riesgos y las buenas prácticas de TI, por ejemplo, pueden integrarse perfectamente en el enfoque de sostenibilidad.

La existencia de estándares y guías sobre el tema también contribuye a brindar mayor claridad y seguridad a las organizaciones en su proceso de transición. No obstante, es crucial reconocer que, para lograr una verdadera transformación hacia la sostenibilidad, es necesario que tanto los archivistas como los profesionales de TI adquieran nuevas habilidades y competencias. Si bien los planes de formación son esenciales, es necesario ir más allá y repensar los programas educativos para preparar a las nuevas generaciones de profesionales para afrontar los retos de la sostenibilidad en el ámbito archivístico.

En definitiva, la incorporación del enfoque de sostenibilidad en la organización archivística requiere un compromiso profundo y sostenido por parte de todos los actores involucrados. Si bien el camino puede ser desafiante, los beneficios a largo plazo son significativos, tanto para la organización en sí como para el medio ambiente y la sociedad en su conjunto.

Bibliografía

Asociación Española de Normalización y Certificación. (2015). *Norma UNE-ISO 14721:2015 Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS) Modelo de referencia.* España: AENOR

BANAT-BERGER F., HUC C., DUPLOUY L., *L'Archivage numérique à long terme, les débuts de la maturité?* (Primera obra de síntesis sobre el archivo digital en lengua francesa) Paris, La Documentation française, 2009

BANAT-BERGER F., HUC C., Module 7 - Gestion et archivage des documents numériques. Portail International Archivistique Francophone. 2011. https://www.piaf-archives.org/se-former/module-7-gestion-et-archivage-des-documents-numeriques (Se identifica en el texto como PIAF)

Digital Information LifeCycle Interoperability Standards Board (DILCIS Board). (14 de 04 de 2024). Digital Information LifeCycle Interoperability Standards Board (DILCIS Board). Obtenido de eArchiving Standards & Specifications: https://dilcis.eu/

DLM FORUM. (14 de 04 de 2024). MoReq: modular requirements for records systems. Obtenido de MoReq2010: https://moreq.info/

Gobierno de España. (14 de 04 de 2024). Política de gestión de documentos electrónicos. Obtenido de Portal administración electrónica: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Archivo_electronico/pae_Politica-de-gestion-de-documentos-electronicos.html

Red de transparencia y acceso a la información. (14 de 04 de 2024). Modelo de Gestión de Documentos y Administración de Archivos (MGD) para la Red de Transparencia y Acceso a la Información (RTA). Obtenido de Guía de Implementación Gerencial– Política de gestión de documentos y archivos: http://mgd.redrta.org/guia-de-implementacion-gerencial-politica-de-gestion-de-documentos-y-archivos/mgd/2015-01-21/124946.html


IBERARCHIVOS
IBERARQUIVOS


ARCHIVO NACIONAL
COSTA RICA


UNIVERSIDAD DE
COSTA RICA