ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

Riesgos y auditoría en la gestión de los documentos electrónicos

Vicent Giménez Chornet

Universitat Politècnica de València

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

Aparición del soporte digital/electrónico/numérico

Preocupación del nuevo soporte de la información

Priorizar en las características adversas o en las ventajosas da argumentos a los detractores o a los seguidores de la sociedad digital

Desde la aparición del documento digital hemos avanzado en dos aspectos:

- 1, en su paulatina introducción en nuestra actividad cotidiana
- 2, en el conocimiento de sus riesgos y cómo afrontarlos

Pero, sin embargo, aún vemos que existen problemas:

¿por qué las administraciones no avanzan en su implementación?

¿a qué se deben los fracasos, reticencias o retrasos en la implementación de una gestión de los documentos electrónicos de archivo?

¿Qué sabemos de los riesgos existentes en la gestión de los documentos electrónicos?

- Riesgos técnicos
- Riesgos de seguridad
- Riesgos legales
- Riesgo económico
- Riesgos institucionales

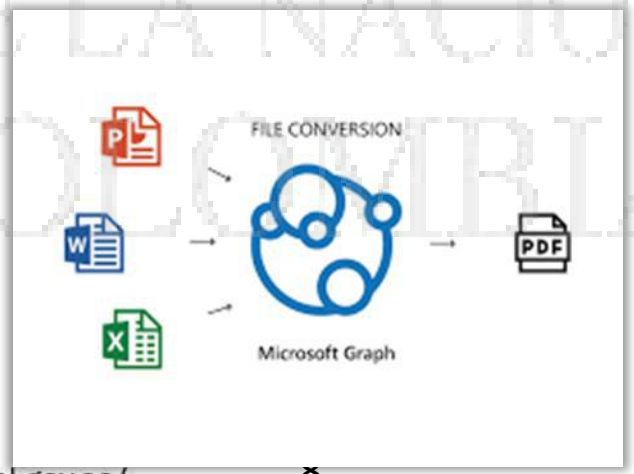
Riesgos técnicos:

En el DLM Forum de 2002 el tema principal era el acceso y preservación de la información electrónica, donde ya se reconocía que

“se necesitan soluciones que garanticen la accesibilidad a largo y corto plazo y la recuperación inteligente del conocimiento almacenado en sistemas de archivos y gestión de documentos”

Riesgo técnico 1: “Captura, indexación y autocategorización”.

Riesgo técnico 2: “Formatos y conversión de documentos”



ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

Riesgo técnico 3: “Gestión de contenidos”

Riesgo técnico 4: “Acceso y protección”

Gestión de usuarios y trazabilidad

Riesgo técnico 5: “Disponibilidad y conservación”

Documentos electrónicos disponibles a lo largo del tiempo, Recomendable seguir:

-ISO 16175 (2010) sobre “*Principios y requisitos funcionales para documentos en entornos de oficina electrónica*”

-ISO/TR 18492: 2005 sobre “*Conservación a largo plazo de información electrónica basada en documentos*”.

Riesgo técnico 6: Los metadatos

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

Riesgo técnico 7: Redes e interoperabilidad

Riesgo técnico 8: Evaluación

Conceptos de retención y disposición

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

Riesgos de seguridad:

Desde la aparición de la red, uno de los principales riesgos es el de la seguridad de los sistemas de información.

Riesgo de seguridad 1: Gestión de riesgos (informáticos)

Riesgo de seguridad 2: Política de Seguridad de la Información (requisitos, servicios y órganos responsables)

Riesgo de seguridad 3: Sistema de Gestión de Evidencias Electrónicas (parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar de manera segura la administración de las evidencias electrónicas)

Riesgos legales:

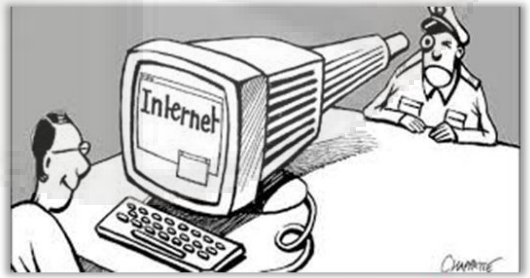
El principal riesgo es la ausencia de una normativa jurídica que respalde la validez de los trámites de los documentos electrónicos.

Riesgo legal 1: - El acceso a la información digital.

Riesgo legal 2: Los derechos de los documentos digitales (propiedad intelectual, patentes y secretos industriales y comerciales.)

Riesgo legal 3: La privacidad.

(datos personales, derecho a saber, olvido digital)



ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

Riesgo legal 4: La transparencia.

Riesgo legal 5: La sede electrónica.

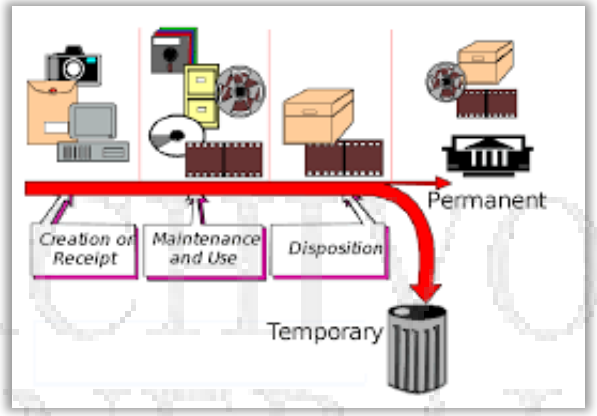
Riesgo legal 6: La firma electrónica.

(Da autenticidad al documento)

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

Riesgo legal 7: La valoración documental.

(regular organismos y funciones)



Riesgo legal 8: La interoperabilidad.

Riesgo legal 8: La reutilización.

Riesgo legal 9: La conservación.

(Regular las estrategias que deben aplicar las organizaciones para garantizar la conservación a corto y largo plazo.)

Riesgo legal 10: La custodia.

(Regular el sistema de transferencias en la administración electrónica, especialmente en los aspectos semánticos y en los técnicos)

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

Riesgo legal 11: El sistema nacional de archivos.

(Correlación jerárquica de los archivos, organismos directivos que impulsen la política archivística nacional.)

Riesgo legal 12: La rendición de cuentas.

(Buena gobernanza)

Las normas jurídicas de buena gobernanza tienen que garantizar la rendición de cuentas a través de una eficaz gestión de los documentos.

Riesgo legal 13: La prestación de servicios.

(regular el catálogo de los servicios públicos, con los derechos y obligaciones de sus usuarios, estructura funcional, competencias, financiación y gestión.)

Riesgo legal 14: La política de gestión de documentos electrónicos.

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

Riesgo económico:

Algunos proyectos de sistemas de gestión de documentos electrónicos se han suspendido o han fracasado por falta de financiación.

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

Riesgos institucionales:

Las organizaciones deben asegurar la sostenibilidad del proyecto a lo largo del tiempo

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

Riesgo institucional 1: Gestión del cambio

(Realizar una gestión del cambio para preparar adecuadamente a las personas.)

Riesgo institucional 2: Desarrollo de capacidades, formación.

Riesgo institucional 3: Gestión de calidad.

Riesgo institucional 4: Cultura corporativa.

(Gestión colaborativa, acceso a la memoria corporativa)

Riesgo institucional 5: Gestión de proyectos.

(Gestionar los recursos, el tiempo y las tareas en unas etapas diferenciadas.)

Riesgo institucional 6: Responsabilidades del equipo de dirección.

Nuevos retos para solucionar nuevos riesgos

Nuevo riesgo: Falta de conciencia de la alta dirección.

Nuevo riesgo: La falta de confianza.

Para disponer de un servicio de confianza cualificado se debe una auditoría externa a la organización.

¿Auditoria?

¿De la contabilidad?

Complejidad de la auditoría en la gestión de documentos

¿Qué perfil debe tener el auditor?

Contexto: auditoría certificada

"La certificación tiene por objetivo general proporcionar confianza a todas las partes de que un sistema de gestión cumple los requisitos especificados. El valor de la certificación reside en el grado de confianza y fe pública que se establece con una evaluación imparcial y competente por una tercera parte"

Norma ISO/IEC 17021-1. *Evaluación de la conformidad. Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión. Parte 1: Requisitos*

Un auditoría certificada puede interesar a:

- Los usuarios
- Las autoridades gubernamentales
- Las organizaciones colaboradoras y contractuales

¿Por qué auditar?

- Asegurar que hacen lo que dicen hacer
- Asegurar que lo que hacen es correcto
- Ayudar a la entidad en las buenas prácticas
- Detectar carencias de alto riesgo

Competencias/habilidades del auditor

- Pensamiento crítico
- Comprensión e integración
- Análisis y resolución de problemas
- Planificación y gestión del tiempo
- Comunicación efectiva
- Habilidades tecnológicas
- Trabajo colaborativo

Conocimientos de quien audita

- Organización de archivos
- Normas técnicas de descripción e indización
- Administración de archivos
- Marco jurídico
- Riesgos y seguridad de la información
- Mercado de la tecnología archivística
- Retos de los archivos en la era digital: redes, administración electrónica, preservación, interoperabilidad, etc.

Principios de quien audita

Imparcialidad: es necesario ser imparcial y ser percibido como imparcial

Riesgos

- Organizaciones conectadas con los gobiernos
- Intereses privados del órgano auditor
- Extorsión por el órgano auditor
- Recursos compartidos

Responsabilidad legal: el órgano auditor debe de ser una entidad legal con funciones de auditoria.

Riesgos:

- Organizaciones alegales
- Organizaciones sin responsabilidades de auditoría
- No tramitar quejas de la auditoría

Competencia: el personal del organismo auditor debe certificar que tiene los conocimientos pertinentes.

Riesgos:

- Falta de entendimiento entre la empresa auditora y el organismo auditado
- Graves carencias en las tareas de la auditoría
- Informes de auditoría ininteligibles

Transparencia: el organismo auditor debe proporcionar acceso público al proceso y los resultados de la auditoría (excepto en la información confidencial).

Riesgos:

- La opacidad es adversa de la confianza
- Desconfianza para atraer organismos colaborativos

Confidencialidad: el organismo auditor debe probar la confidencialidad (por su trayectoria y por la firma de un documento de confidencialidad) para tener acceso privilegiado a la información.

Riesgos:

- Divulgación de información restringida
- Apropiación de información privilegiada

Receptividad (respuesta oportuna a las quejas): el organismo auditor debe tratar adecuadamente las opiniones y quejas para demostrar su integridad y credibilidad a la comunidad.

Riesgos:

- La ausencia en el tratamiento de las quejas promueve acciones discriminatorias
- El proceso de auditoría podría adolecer de errores

¿Que se audita?

- Cuestiones técnicas
- Cuestiones de la organización
- Cuestiones de seguridad
- Cuestiones legales
- Cuestiones económicas
- Cuestiones de recursos humanos
- Tercerización

Lectura aconsejable: ISO 16363:2017 Auditoría y certificación de repositorios digitales de confianza.

Cuestiones técnicas

- Clasificación multinivel
- Descripción normalizada: contenido y productores
- Indización con lenguajes documentales: tesauros
- Valoración documental: retención, disposición, calendarios
- Software de gestión
- Criterios de digitalización: copia máster y de difusión
- Recuperación de la información
- Transferencias
- Redes de archivos

Cuestiones de la organización/entidad

- Responsabilidades: alta dirección, técnicos archiveros, etc.
- Políticas y directrices de la entidad archivística
- Código ético
- Responsabilidad social
- Plan de innovación

Cuestiones de seguridad

- Sistema de seguridad de la información
- Directrices de preservación/conservación de la información
- Plan de prevención de desastres
- Infraestructura adecuada
- Accesos
- Trazabilidad

Cuestiones legales

- Cumplimiento del marco jurídico en archivística
- Protección de los derechos de autor y patentes
- Transparencia
- Reutilización de la información

Cuestiones económicas

- Financiación garantizada
- Auditoría económica: minimizar riesgo financiero
- Sostenibilidad: planificación a corto y largo plazo

Cuestiones de recursos humanos

- Personal adecuado en formación y habilidades
- Carrera profesional
- Formación continua
- Dedicación y remuneración

Tercerización (*outsourcing*)

- Contratación: derechos transferidos, responsabilidades y expectativas de las partes.
- Garantías y solvencia
- Subcontratación: costos y derechos (privacidad, etc.)
- Transparencia
- Valor económico de los servicios: garantizar competencia del mercado, cualitativa y cuantitativamente
- Evaluación de resultados

¡Muchas gracias!

A vuestra disposición en:

vigicho@har.upv.es