CCIL

II Congreso sobre Control Interno Local

"Estrategias para un ejercicio eficaz del Control Interno"

21 y 22 de octubre

Palacio de Congresos de Huesca

DIPUTACIÓN DE HUESCA

GOBIERNO DE ESPAÑA · MINISTERIO DE HACIENDA · IGAE · INTERVENCIÓN GENERAL DE LA ADMINISTRACIÓN DEL ESTADO

Los sistemas de información dentro de los procesos de control financiero permanente y auditoría pública.

Moderador: Antonio Minguillón Roy
Ponente: Vanessa González San Julián

DIPUTACIÓN DE HUESCA

GOBIERNO DE ESPAÑA · MINISTERIO DE HACIENDA · IGAE · INTERVENCIÓN GENERAL DE LA ADMINISTRACIÓN DEL ESTADO

Moderador: Antonio Minguillón Roy

minguillon_ant@gva.es

DIPUTACIÓN DE HUESCA

GOBIERNO DE ESPAÑA · MINISTERIO DE HACIENDA · IGAE · INTERVENCIÓN GENERAL DE LA ADMINISTRACIÓN DEL ESTADO

CCIL II Congreso sobre Control Interno Local

Los retos de la auditoría pública en la era de la administración electrónica

Antonio Minguillón Roy

SINDICATURA DE COMPTES

minguillon_ant@gva.es

Tecnología de complejidad creciente

Ciberseguridad

VICEPRESIDENCIA SEGUNDA
DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

PROYECTO DE REAL DECRETO POR EL QUE SE REGULA EL ESQUEMA NACIONAL DE SEGURIDAD

Durante todo este periodo, la transformación digital de las Administraciones públicas españolas, y del sector público en general, ha progresado significativamente, suponiendo una mejora en la prestación de sus servicios y un mayor acercamiento a los ciudadanos. Ahora bien, la transformación digital también ha supuesto un incremento de los riesgos asociados a los sistemas de información que sustentan los servicios públicos y, por tanto, a la información que manejan. El Sector Privado está igualmente inmerso en la transformación digital de sus procesos de negocio, de forma que sus sistemas de

De hecho, desde entonces, se ha evidenciado que los sistemas de información están expuestos de forma cada vez más intensa a la materialización de amenazas del ciberespacio, a los ciberincidentes, que siguen una pauta de crecimiento en frecuencia, sofisticación, alcance y severidad del impacto. Diversos organismos internacionales y del ámbito de la Unión Europea, así como las sucesivas estrategias de ciberseguridad, de 2013 y, particularmente la Estrategia Nacional de Ciberseguridad 2019, reconocen que los ciberincidentes que se materializan en los sistemas de información de las organizaciones constituyen una de las amenazas más significativas para el normal desenvolvimiento de las sociedades, instituciones, empresas y ciudadanos. La evolución de las amenazas, los

Transformación digital y ciberseguridad

Qué es la transformación digital de la administración

La transformación digital no es una cuestión exclusivamente técnica, no es la mera informatización de procesos administrativos tradicionales. Implica partir de cero y reflexionar sobre cuál es la mejor forma de prestar un servicio con los medios tecnológicos actuales. Es decir, la tecnología solo es un elemento instrumental para llevar a cabo la reingeniería de procesos que implica la transformación digital de la Administración. Por tanto, la mera incorporación de la tecnología no puede hacer buenos unos procedimientos obsoletos.

Por otra parte, la total dependencia de los sistemas de información y de comunicaciones existente en la gestión pública hace que las Administraciones públicas sean más vulnerables frente a los ciberataques, de modo que la transformación digital debe ir inseparablemente unida a la ciberseguridad.

Auditoría de Sistemas de Información y RD 424/2017

Artículo 6. *De las facultades del órgano de control.*

1. El órgano interventor podrá hacer uso en el ejercicio de sus funciones de control del deber de colaboración, de la facultad de solicitar asesoramiento, de la defensa jurídica y de la facultad de revisión de los sistemas informáticos de gestión de acuerdo con lo previsto en los párrafos siguientes.

4. Cuando la naturaleza del acto, documento o expediente lo requiera el órgano interventor de la Entidad Local, en el ejercicio de sus funciones de control interno, podrá recabar directamente de los distintos órganos de la Entidad Local los asesoramientos jurídicos y los informes técnicos que considere necesarios, así como los antecedentes y documentos precisos para el ejercicio de sus funciones de control interno, con independencia del medio que los soporte.

7. Los funcionarios actuantes en el control financiero podrán revisar los sistemas informáticos de gestión que sean precisos para llevar a cabo sus funciones de control.

Artículo 30. *Obtención de información, documentación y asesoramiento técnico en las actuaciones de control financiero.*

1. En el ejercicio de las funciones de control financiero se deberán examinar cuantos antecedentes, documentación e información sean precisos a efectos de las actuaciones de control, así como consultar la información contenida en los sistemas informáticos de gestión que sea relevante.

3. El órgano interventor responsable de la ejecución del control financiero podrá solicitar de los órganos y entidades objeto de control la documentación contable, mercantil, fiscal, laboral y administrativa o de otro tipo que se considere necesaria para el desarrollo de las actuaciones, ya sea en soporte documental o en programas y archivos en soportes informáticos compatibles con los equipos y aplicaciones del órgano de control, y el acceso para consultas a los sistemas y aplicaciones que contengan información económico-financiera del órgano, organismo o entidad controlada.

4. Las actuaciones de obtención de información podrán iniciarse en cualquier momento una vez notificado el inicio del control sin que se precise previo requerimiento escrito.

5. En ningún caso el órgano interventor tendrá la obligación de procurarse por sí mismo la documentación e información directamente de los archivos físicos y de las aplicaciones y bases de datos informáticas, sin perjuicio de que se pueda utilizar este procedimiento cuando los auditores y los responsables de la entidad lo acuerden y siempre que la documentación sea fácilmente accesible.

CAPÍTULO III

De la auditoría pública

Artículo 33. *Ejecución de las actuaciones de auditoría pública.*

4. Para la aplicación de los procedimientos de auditoría podrán desarrollarse las siguientes actuaciones:

e) Verificar la seguridad y fiabilidad de los sistemas informáticos que soportan la información económico-financiera y contable.

f) Efectuar las comprobaciones materiales de cualquier clase de activos de los entes auditados, a cuyo fin los auditores tendrán libre acceso a los mismos.

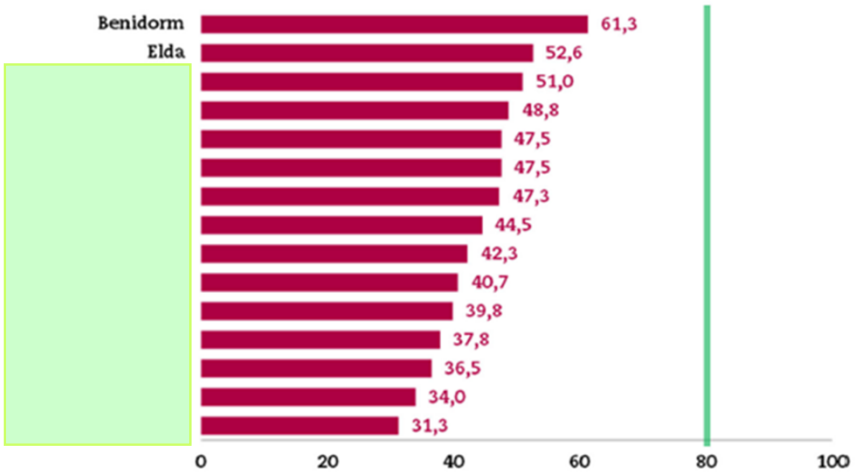
¡es una exigencia legal también para los EELL!

RESUMEN

Los sistemas de información analizados están en riesgo frente a las amenazas de ciberseguridad

Ninguno de los ayuntamientos auditados alcanza el índice de madurez de los controles básicos de ciberseguridad del 80% requerido por el ENS (es decir, solo se puede considerar haber obtenido un "aprobado" en ciberseguridad alcanzando la línea verde del gráfico).

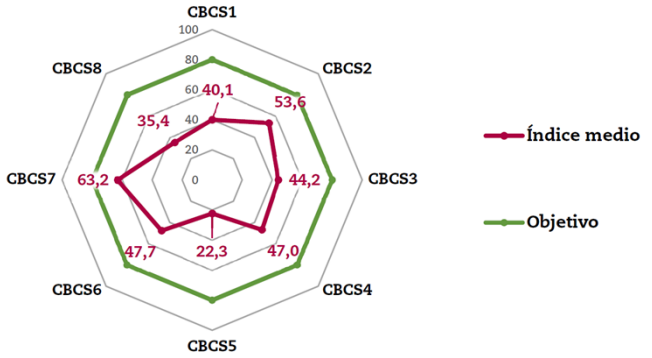
Bajo índice de madurez de los CBCS



En general, el nivel de cumplimiento con la normativa relacionada con la seguridad de la información es bastante insatisfactorio

IM medio= 44,2%

Gráfico 2. Índice medio de madurez de los CBCS



El ENS y las auditorías

En el actual entorno de administración electrónica,

el cumplimiento con el ENS adquiere una gran trascendencia

y los auditores del sector público deberán verificar el

cumplimiento de la legalidad en relación con el ENS y

si no se acredita la adecuación al mismo se debería reflejar en el informe como un incumplimiento grave o muy significativo.

ORGANIZADORES

DIPUTACIÓN DE HUESCA

GOBIERNO DE ESPAÑA · MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA · IGAE INTERVENCIÓN GENERAL DE LA ADMINISTRACIÓN DEL ESTADO

COLABORADORES

Ayuntamiento de Huesca

COSITAL Secretarios, Interventores y Tesoreros de Administración Local Consejo General

COSITAL network | Proyecto Esperanto
www.cositalnetwork.es

PATROCINADORES

Oro

SPAI innova

audifilm GRUPO AL

Plata

FAURA-CASAS AUDITORS-CONSULTORS

T-Systems

Berger Levrault

CON EL APOYO E IMPULSO DE Wolters Kluwer

Los sistemas de información dentro de la innovación de los procesos de control financiero permanente y auditoria pública

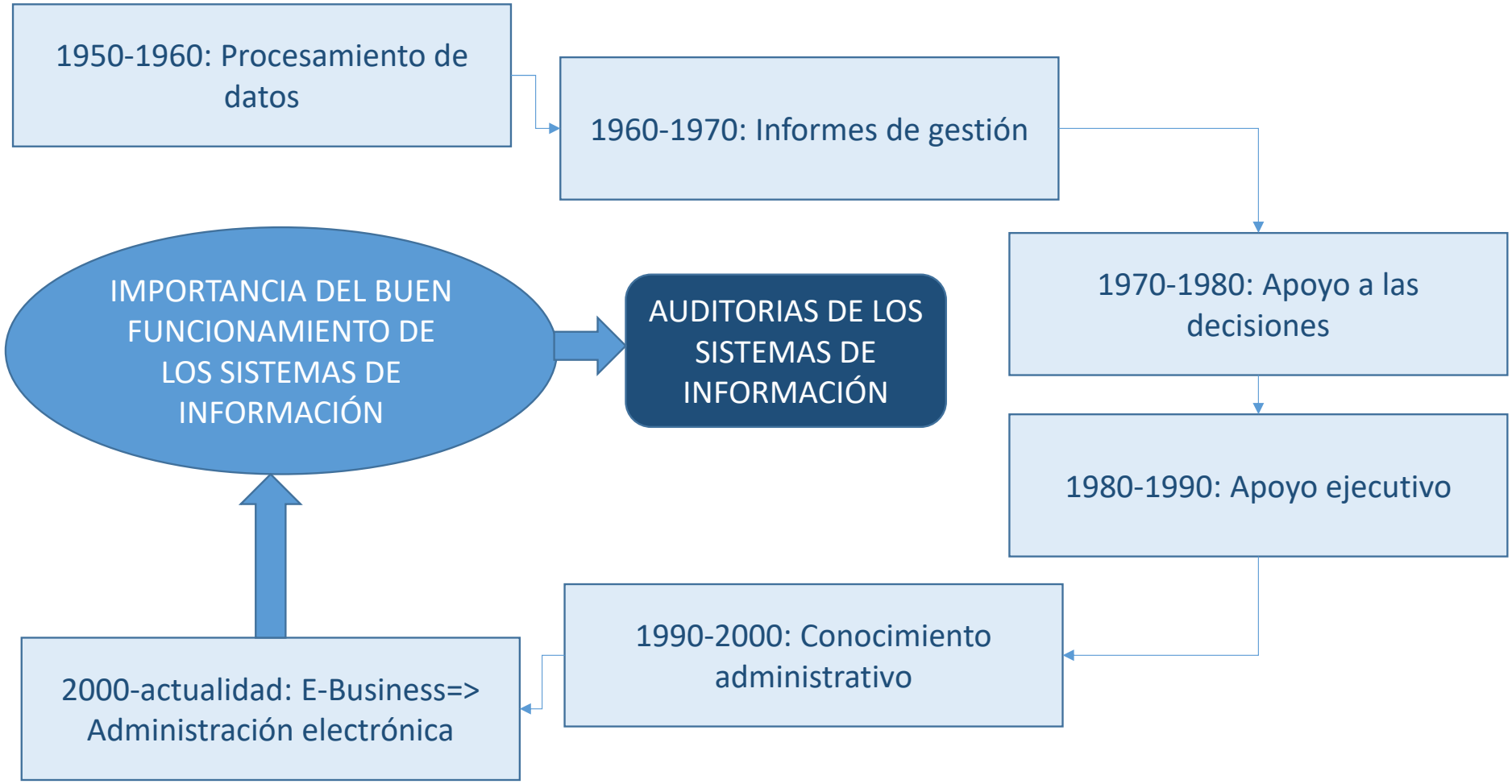
Vanessa González San Julián

vgonzalez@igae.hacienda.gob.es

DIPUTACIÓN DE HUESCA

GOBIERNO DE ESPAÑA · MINISTERIO DE HACIENDA · IGAE INTERVENCIÓN GENERAL DE LA ADMINISTRACIÓN DEL ESTADO

Introducción: los sistemas de información como base de los procesos de negocio dentro de una organización



Importancia del análisis de datos dentro del proceso de auditoría

El Equipo de Auditoría Informática (EAI) de la IGAE

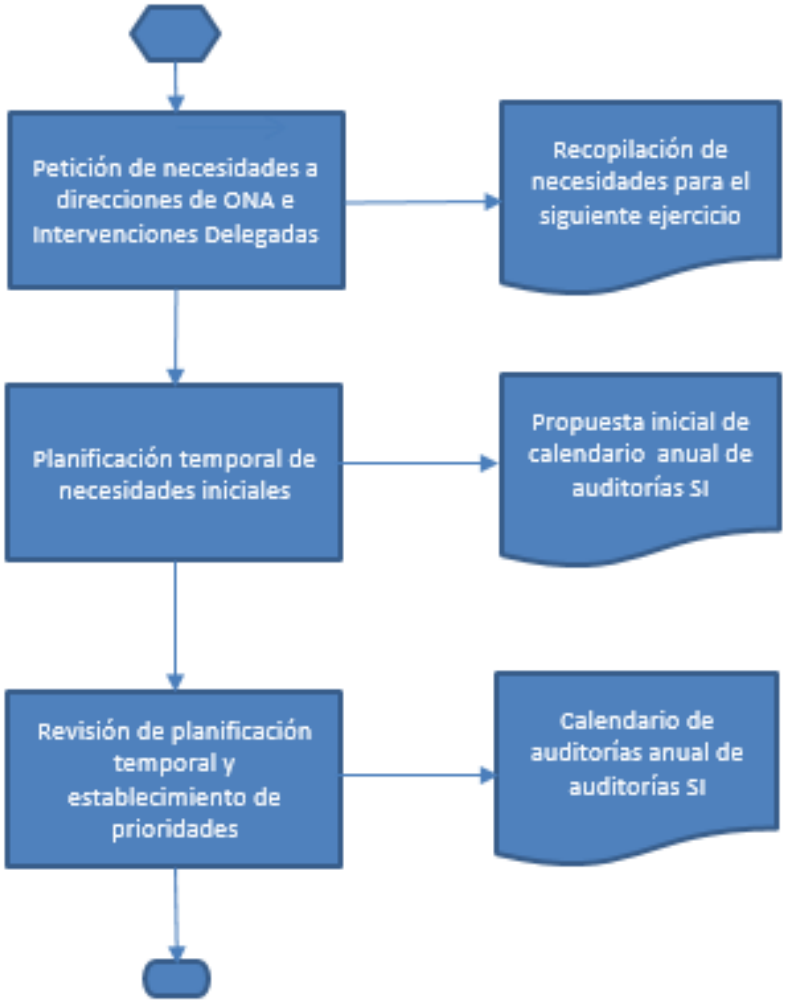
El equipo de auditoría informática se crea en el año 2008. Está compuesto por un reducido número de personas que acumulan experiencia en diversos campos de las TIC, desde el desarrollo hasta la operación.

Real Decreto 682/2021, de 3 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Función Pública. El artículo se detallan las funciones de la Oficina de Informática Presupuestaria en relación con auditorías de sistemas de información:

"La colaboración con la Oficina Nacional de Auditoría en la realización de auditorías y de asesoramientos de naturaleza informática que, en relación con los controles financieros, le sean asignados por el Director de la Oficina, y el control interno de calidad de los sistemas desarrollados por la Oficina de Informática Presupuestaria".

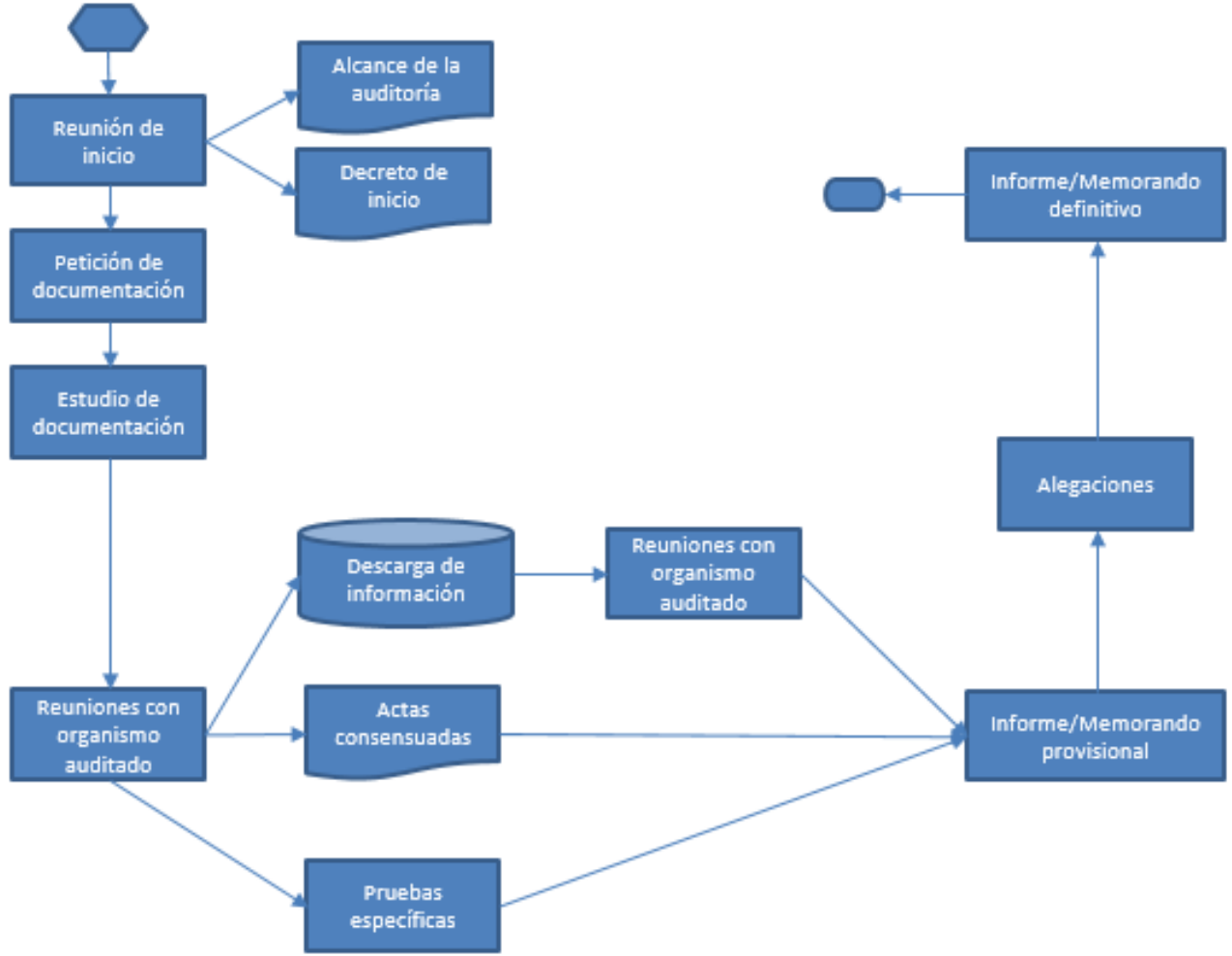
Importancia del análisis de datos dentro del proceso de auditoría

Metodología de trabajo: plan anual de auditorías



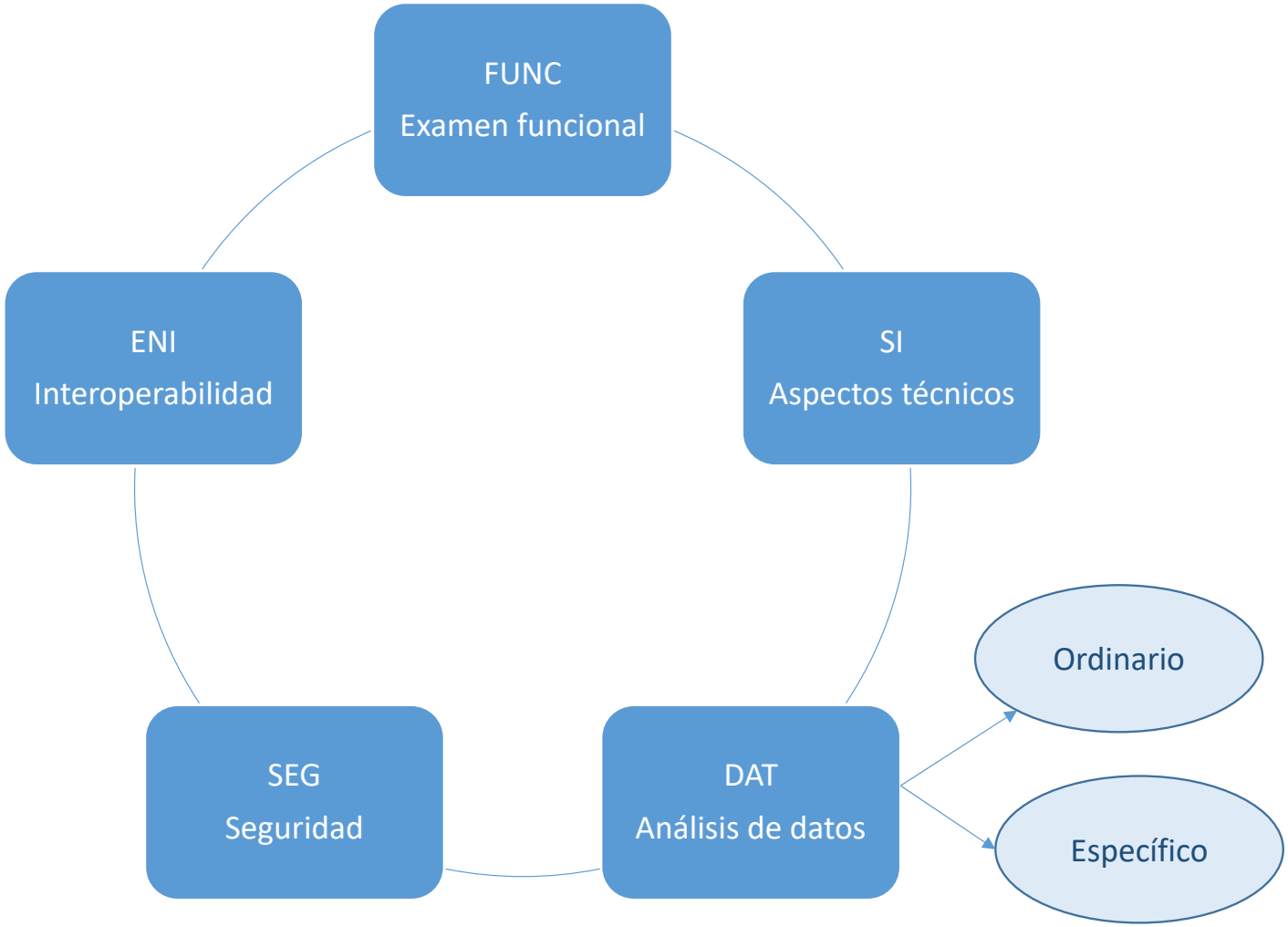
Importancia del análisis de datos dentro del proceso de auditoría

Metodología de trabajo: desarrollo de una auditoría



Importancia del análisis de datos dentro del proceso de auditoría

Controles dentro de una auditoría



Importancia del análisis de datos dentro del proceso de auditoría

Controles dentro de una auditoría

Control	Descripción
FUNC.1: Entorno organizacional	Revisión de aspectos organizativos de la entidad responsable del sistema o sistemas de información en estudio.
FUNC.2: Descripción de los procesos de negocio	Revisión del proceso de negocio asociado a los objetivos de control. En este control se analiza el flujo de información entre los diferentes sistemas involucrados desde un punto de vista teórico, detectando posibles debilidades en el traspaso de la información

Control	Descripción
SI.1: Verificación de aspectos de la arquitectura de sistemas	Se revisan diferentes aspectos relacionados con la arquitectura de sistemas que da soporte al sistema o sistemas de información relacionados con el proceso de negocio que se está estudiando. Se analizará entre otros las redes de comunicación, infraestructura de servidores, seguridad de los elementos que forman parte de la arquitectura.
SI.2: Verificación de aspectos relacionados con el proceso de desarrollo.	Se estudia el proceso de desarrollo software de los sistemas de información implicados en los objetivos de control. Entre otros, se analizará metodología de desarrollo empleada, tecnología, versiones de productos, estándares, seguridad dentro del proceso de desarrollo.
SI.3: Verificación de aspectos relativos a la gestión del servicio.	En caso de que el desarrollo o la operación de sistemas de información relacionados con el objetivo de control se lleve a cabo por proveedores externos, se revisará el contrato establecido, analizando entre otros vigencia del mismo o acuerdos de nivel de servicio.
SI.4: Verificación de aspectos relativos a la gestión del conocimiento y formación	Dentro de este control se revisará las labores de gestión del conocimiento y formación necesarias en la administración y operación del sistema o sistemas de información implicados en los objetivos de control.

Importancia del análisis de datos dentro del proceso de auditoría

Controles dentro de una auditoría

Control	Descripción
DAT.ORD.1: Verificación de aspectos relativos a la calidad del dato.	En este control, se revisará la calidad del conjunto de datos en estudio a través de herramientas especializadas. Entre otras pruebas se comprobará corrección de NIFs, fechas, cuentas bancarias…
DAT.ORD.2: Coherencia y cohesión de los flujos de información.	En caso de que se produzca un flujo de datos entre diferentes sistemas de información implicados en los objetivos de control, se analizará a través de herramientas especializadas la trazabilidad, coherencia y cohesión del conjunto de datos en estudio.
DAT.ORD.3: Verificación del proceso de firma electrónica.	Será necesario realizar pruebas dentro de este apartado si los sistemas de información asociados a los objetivos de control utilizan mecanismos y herramientas propios para firmar electrónicamente, con el objetivo de verificar si dicho proceso es correcto.
DAT.ORD.4: Pruebas analíticas.	En algunos casos, se determinará la necesidad de realizar pruebas analíticas sobre parte del conjunto de datos en estudio, con el objetivo de detectar posibles casos de fraude (ej. Ley de Benford, NDT- Test de duplicación de números…).

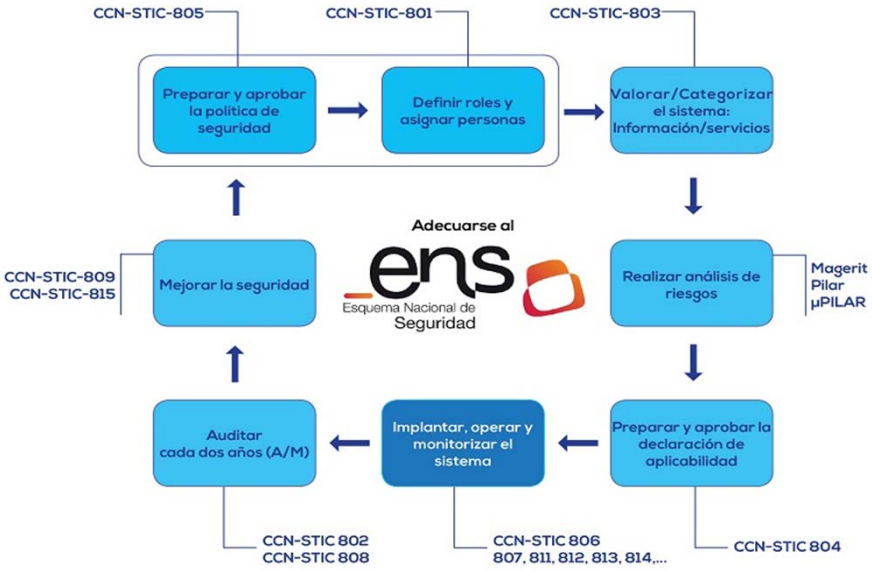
Control	Descripción
SEG.GES: Gestión de la seguridad de la información	Dentro de esta sección y dependiendo de la auditoría se revisará de forma total/parcial clausulas/controles asociados a diferentes estándares de gestión de la seguridad de la información (ISO 27001 o ENS- Esquema Nacional de Seguridad).
SEG.TEC: Pruebas técnicas	En algunos casos, será necesario realizar pruebas técnicas de seguridad como pentesting/hacking ético sobre aplicaciones web o revisión de configuración de sistemas empleando herramientas especializadas (ej. CLARA) con el objetivo de verificar los niveles de seguridad de los sistemas de información implicados en los objetivos de control.

Seguridad dentro de los sistemas de información:

Gestion de la seguridad

- **ISO 27001:** norma internacional que permite asegurar entre otros la confidencialidad e integridad de los datos. Se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

- **ENS (RD 3/2010 actualizado en 951/2015): s**erie 800 ENS - https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html



Seguridad dentro de los sistemas de información:

Guía CCN-STIC-808: Verificación del cumplimiento de las medidas del ENS

- Sistemas de nivel **BASICO**: autoevaluación con declaración de conformidad cada 2 años / en caso de modificaciones sustanciales del sistema. La autoevaluación podrá ser desarrollada por el mismo personal que administra el sistema de información o en quién éste delegue.
- Sistemas de nivel **MEDIO o ALTO**: auditoría formal cada dos años / en caso de modificaciones sustanciales del sistema. Se realizará por una entidad de certificación acreditada por la ENAC o por aquellas entidades, órganos, organismos y unidades vinculadas o dependientes de las Administraciones Públicas que cumplan los requisitos fijados (resolución 13/10/2016, CCN-STIC 122).

Aptdo.	Categoría	Requisito	Aplicabilidad - Auditado	Comentarios
org	*MARCO ORGANIZATIVO*			
org.1	*Política de seguridad*			
	Básica	☐ 1.- ¿Dispone de una política de seguridad escrita? *Evidencia: La política de seguridad está impresa o guardada en formato electrónico.* Respecto a dicha política de seguridad: ☐ 1.1.- ¿Ha sido aprobada por el órgano superior competente (de acuerdo a lo establecido en el artículo 11 del RD 3/2010)? *Evidencia: La política de seguridad fue redactada por un órgano superior o ha sido aprobada (mediante algún registro escrito o electrónico) por el mismo. En caso de que el órgano superior no disponga de política de seguridad, deberá tener una política de seguridad elaborada por el responsable STIC y aprobada por el Comité STIC y el Comité de Seguridad Corporativa. Además, existe un procedimiento de revisión y firma regular (este último si no existe una política de seguridad redactada por un órgano superior).*	Aplica: ☐ Sí Lo audito: ☐ Sí	Registros: ☐ Documento: ☐ Muestreo: Observaciones auditoría:

Seguridad dentro de los sistemas de información:

Auditorías de ciberseguridad

En algunos casos será necesario realizar pruebas técnicas de seguridad para comprobar las posibles vulnerabilidades del sistema o sistemas de información relacionados con los procesos de negocio analizados dentro de la auditoría que se está llevando a cabo.

Algunas pruebas que se pueden realizar:

- Pentesting de aplicaciones web (metodología OWASP)
- Análisis de configuración de seguridad con la herramienta CLARA.
- Análisis de protocolos de comunicación.

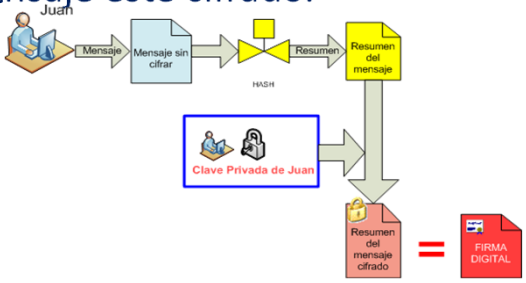
Mecanismos para verificar las dimensiones de seguridad de documentos electrónicos dentro del contexto de una auditoría

✓ **Huella digital:** verificación de integridad y no repudio.

Conjunto de datos asociados a un mensaje que permiten asegurar que el mensaje no fue modificado (=>**no repudio de los documentos**). Se obtiene aplicando una función, denominada hash, a ese mensaje, lo que da como resultado un conjunto de datos singular de longitud fija.

✓ **Firma digital:** verificación de la identidad del firmante e integridad del mensaje

Conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje. No implica que el mensaje esté cifrado.



VALIDe

https://valide.redsara.es/valide/?

✓ **Sellado de tiempo:** verificación de integridad de información en un momento determinado

El sellado de tiempo es un método para probar que un conjunto de datos existió antes de un momento dado y que ninguno de estos datos ha sido modificado desde entonces.

Plataforma de Sellado de Tiempo TS@ (https://administracionelectronica.gob.es/ctt/tsa#.X4SSiJgzaUk)

ORGANIZADORES

DIPUTACIÓN DE HUESCA

GOBIERNO DE ESPAÑA · MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA · IGAE INTERVENCIÓN GENERAL DE LA ADMINISTRACIÓN DEL ESTADO

COLABORADORES

Ayuntamiento de Huesca

COSITAL Secretarios, Interventores y Tesoreros de Administración Local Consejo General

COSITAL network | Proyecto Esperanto
www.cositalnetwork.es

PATROCINADORES

Oro

SPAI innova

audifilm GRUPO AL

Plata

FAURA-CASAS AUDITORS-CONSULTORS

T-Systems

Berger Levrault

CON EL APOYO E IMPULSO DE Wolters Kluwer