
PRIORIDADES TIC EN LA DIPUTACIÓN DE SALAMANCA

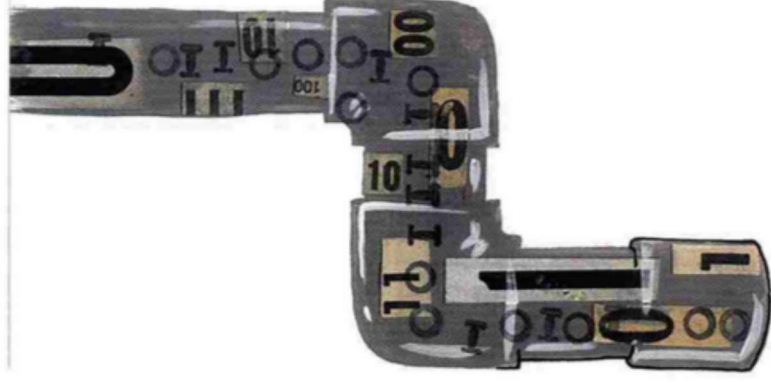
Francisco Javier Delgado Álvarez

Jefe de Proyecto del Área de Informática Corporativa

OA CIPSA – Diputación de Salamanca

1.¿"IT doesn't matter"?

“IT Doesn't Matter”, Nicholas Carr, Harvard Business Review, May-2003



HBR AT LARGE

IT Doesn't Matter

by Nicholas G. Carr

As information technology's power and ubiquity have grown, its strategic importance has diminished. The way you approach IT investment and management will need to change dramatically.

1.¿"IT doesn't matter"?

“IT Doesn't Matter”, Nicholas Carr, Harvard Business Review, May-2003

¿SON IRRELEVANTES LAS TIC EN NUESTRAS ADMINISTRACIONES PÚBLICAS?

- Ubicuidad de las “nuevas tecnologías” y pérdida de valor estratégico.
 - Pasado: Energía eléctrica y ferrocarril.
 - Presente: Tecnologías de la Información y la Comunicación.
 - Futuro: ¿Inteligencia artificial?
- Los riesgos que conlleva la utilización masiva superan sus ventajas.
 - Necesidad de Gestión de Riesgos: técnicos, organizativos y legales.
- Conversión suministradores de productos en prestadores de servicios.
 - Transformación hacia modelos de suscripción de servicios.
 - ¿Desaparición de las TIC en las organizaciones/administraciones?

2. Las nuevas TIC en la Administración Pública

Nuevas tecnologías en las Tecnologías de la Información y Comunicación

TECNOLOGÍAS EN LA NUBE

- Software/Plataforma/Infraestructura como Servicio: SaaS, PaaS, IaaS.
- Clouds Públicos (AWS, GCP, Azure) o Comunitarios (SARA en AAPP).

NUEVAS TECNOLOGÍAS TIC

- IPv6, 5G, DVI, GPON.
- Autoconfigurables, autoreparables y autogestionados.

SERVICIOS SOPORTE TIC

- Del “despotismo ilustrado TIC” a la “democratización”: *Shadow IT*.
- Publicación webs, almacenamiento, bases de datos, aplicaciones...

SERVICIOS TIC, SIN TICS

- Niveles de riesgo tecnológicos y normativos superiores.
- Más importante qué hacer, que cómo hacerlo o dónde hacerlo.

2. Las nuevas TIC en la Administración Pública

Tecnologías de la Información SIN Tecnologías de la Información

¡ESA SITUACIÓN ES EVIDENTEMENTE IMPOSIBLE!... ¿O ES POSIBLE?

- Velocidad de implantación: el COVID-19.
- Administraciones YA sin apenas infraestructura TIC.

ESCENARIOS EN LOS QUE LAS TIC SON [CASÍ] “IRRELEVANTES”

- Pequeños Ayuntamientos.
- Administraciones de cualquier tamaño apoyadas en *clouds*.

PEQUEÑOS AYUNTAMIENTOS: LA PROVINCIA DE SALAMANCA

- 362 municipios, solo la capital más de 20.000 habitantes.
- 90% municipios por debajo de 1.000 habitantes.
- 60% municipios por debajo de 250 habitantes.
- Recursos disponibles:
 - Secretario-Interventor, un puesto de trabajo y [casí] banda ancha.
 - Aplicaciones locales y servicios en la nube.

2. Las nuevas TIC en la Administración Pública

Prioridades TIC en Administraciones Públicas sin [apenas] TICs

MINIMO COMÚN ELEMENTO QUE COMPARTEN TODAS LAS ADMINISTRACIONES

- Independientemente del tamaño o intensidad de uso de las TIC:
 - Seguridad técnica,
 - Seguridad jurídica.

ELEMENTOS CATALIZADORES PARA LA TRANSFORMACIÓN DIGITAL DE AAPP

- Reglamento General de Protección de Datos (RGPD).
- Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Esquema Nacional de Seguridad (ENS).

OBJETIVOS

- Servir de ayuda para el aprovechamiento eficaz y seguro de las TIC para mejorar el desempeño en el ejercicio de sus competencias para el beneficio de los ciudadanos.

3. APLICACIÓN DEL ENS Y DEL RGPD+LOPDGDD

Esquema Nacional de Seguridad (RD 3/2010, modificado por RD 951/2015)

ESTABLECER PRINCIPIOS BÁSICOS Y REQUISITOS MÍNIMOS DE LA SEGURIDAD GESTIÓN DE LA SEGURIDAD BASADA EN RIESGOS CATÁLOGO DE MEDIDAS DE SEGURIDAD SEGÚN CATEGORÍA SISTEMA INFORM. DIFERENTES FIGURAS CON RESPONSABILIDADES EN APLICACIÓN DEL ENS

- Responsable de Seguridad (RSEG), Responsable de la Información, Responsable del Servicio, Responsable del Sistema.

FUNCIONES DEL RESPONSABLE DE SEGURIDAD (RSEG)

- Mantener seguridad información manejada y servicios prestados.
- Auditorías para verificar cumplimiento ENS.
- Formación y concienciación seguridad.
- Verificar adecuación medidas de seguridad.
- Monitorizar estado de la seguridad.
- Apoyar y supervisar investigación incidentes de seguridad.

3. APLICACIÓN DEL ENS Y DEL RGPD+LOPDGDD

RGPD (Reglamento 2016/679) y LOPDGDD (LO 3/2018)

ORIENTACIÓN AL RIESGO

MEDIDAS DE SEGURIDAD SIN CONCRETAR (ISO 27001 Y ENS)

FIGURAS CON RESPONSABILIDADES APLICACIÓN RGPD+LOPDGDD

- Responsable del Tratamiento (RT).
- Encargado del Tratamiento (ET).
- Delegado de Protección de Datos (DPD).

FUNCIONES DEL DELEGADO DE PROTECCIÓN DE DATOS (DPD)

- Informar y asesorar al RT/ET y empleados de aspectos protección datos.
- Supervisar cumplimiento protección de datos, formación y auditorías.
- Ofrecer asesoramiento Evaluación Impacto Protección de Datos (EIPD).
- Cooperar con Autoridad de Control (AEPD).
- Punto de contacto AC y titulares de los datos.

3. APLICACIÓN DEL ENS Y DEL RGPD+LOPDGDD

RELACIONES ENTRE EL ENS Y RGPD+LOPDGDD

LOPDGDD

- DA 1ª: RT artículo 77.1 (AAPP) aplicarán medidas previstas ENS.
- ET por cuenta de RT artículo 77.1 también aplicarán medidas ENS.
- Modificación ENS según criterios determinación del riesgo art. 32 RGPD.

ENS

- Medida “mp.info.1 – Datos de carácter personal”: legislación protección de datos como medida de protección entre las enumeradas Anexo II.
- Guía CCN-STIC-881 Impacto del RGPD en el ENS (pendiente).
- Consejo de Ministros 25/5, actualización ENS por vía urgencia (RDL).
- Efecto futura regulación europea NIS2 sustituirá a NIS (no aplica AAPP).

NIS

- Trasposición en España por el RDL 12/2018 y desarrollado RD 43/2021.
- NIS sí aplica, entre otros, a proveedores de servicios *cloud*.

3. APLICACIÓN DEL ENS Y DEL RGPD+LOPDGDD

RELACIONES ENTRE EL RSEG (ENS) Y EL DPD (RGPD+LOPDGDD)

AEPD (INFORME 170/2018)

- Incompatibilidad entre funciones RSEG y DPD
- Perfil RGSEG tecnológico, perfil DPD además conocimiento jurídico.
- EXCEPCIONALMENTE sería admisible en determinados supuestos:
 - Organizaciones, según su tamaño y recursos disponibles.
 - Concurrencia de requisitos de formación y capacitación DPD+RSEG.
 - Medidas garantizar independencia y ausencia conflicto de intereses.
 - Documentar motivadamente la designación concurrente DPD+RSEG.

CCN (GUÍA CCN-STIC-801 “ENS. RESPONSABILIDADES Y FUNCIONES”)

- AEPD señala la posibilidad de coincidencia DPD y RSEG con condiciones.
- ##### **JUSTIFICACIÓN POSIBLE CONCURRENCIA FIGURAS DPD+RSEG**
- Seguridad (ISO 27000 y ENS) en esquema certificación DPD de la AEPD.
 - RSEG+DPD en organizaciones significativas. También Comités conjuntos.

4. ASISTENCIA DIPUTACIONES A AYUNTAMIENTOS

ASISTENCIA TÉCNICA DE LAS DIPUTACIONES A PEQUEÑOS AYTOS.

LEY 7/85, DE 2 DE ABRIL, REGULADORA DE LAS BASES DE RÉGIMEN LOCAL

- Artículo 36.1: Corresponde a las Diputaciones Provinciales:
 - b) La asistencia y cooperación jurídica y técnica a los Municipios, especialmente a los de menor capacidad económica y de gestión.
 - g) La prestación de los servicios de administración electrónica [...] en los municipios con población inferior a 20.000 habitantes.

AEPD

- Servicio de DPD prestado desde las Diputaciones.

ENS

- Art. 11: Política de seguridad elaborada por la Diputación (¿y RSEG?).

ENS / RGPD+LOPDGDD

- Oportunidad desarrollo ordenado de las TIC en las administraciones.
- ¿ Plan Director/Programa [Provincial] de Ciberseguridad y Privacidad ?

4. ASISTENCIA DIPUTACIONES A AYUNTAMIENTOS

PROBLEMAS APLICAR ENS Y RGPD+LOPDGDD EN PEQUEÑOS AYTOS.

ENS

- Designación/nombramiento: RSEG. RSERV, RINF, RSIS.

RGPD+LOPDGDD

- Designación/nombramiento: DPD.

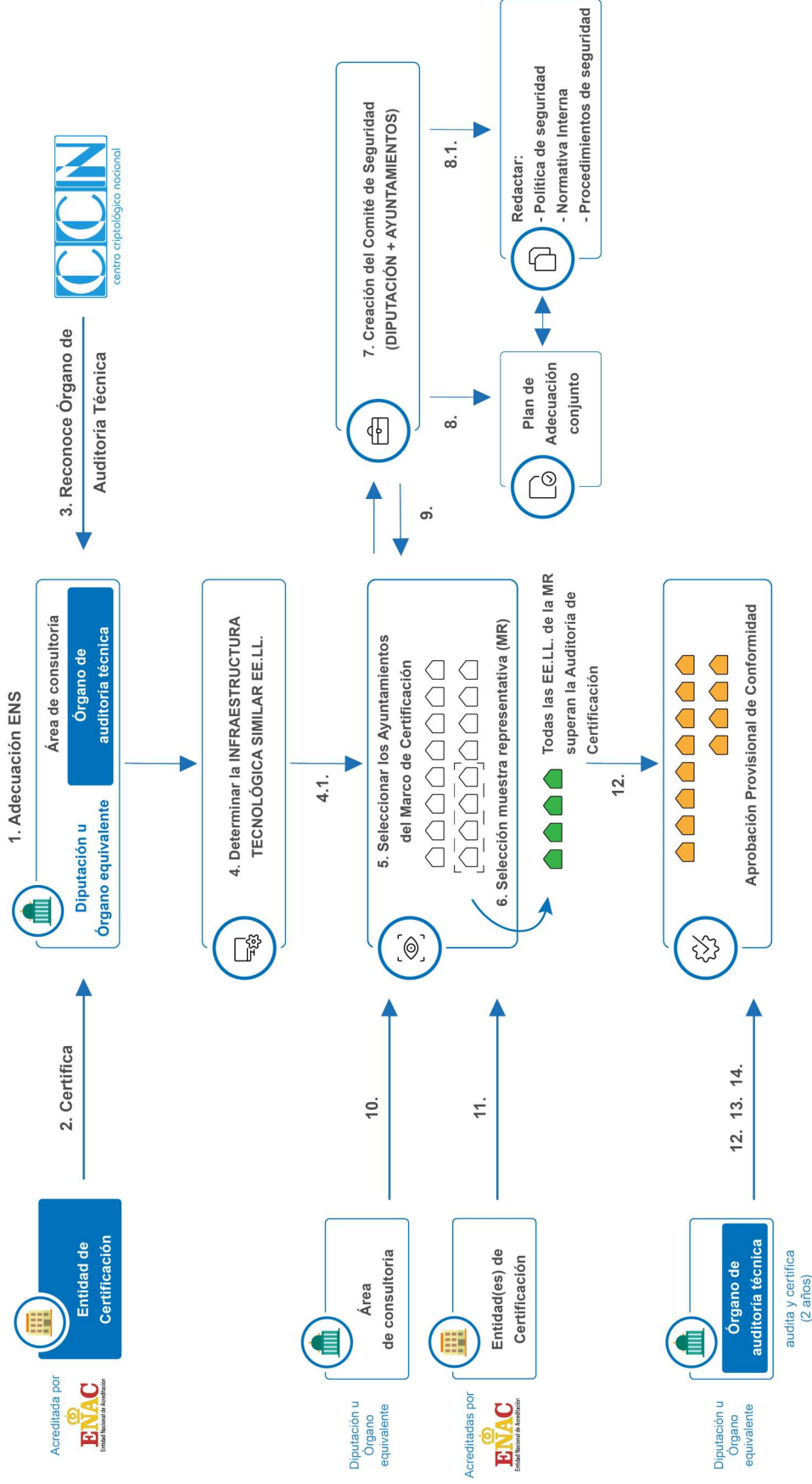
COMO DEBE SER APLICACIÓN SIMULTÁNEA ENS Y RGPD+LOPDGDD

- Proporcional a los riesgos, manteniendo garantías de protección.
- Aplicación sensata, sostenible, sencilla, escalable y coherente.
- Debe aportar valor a la transformación digital de las administraciones.
- CCN reconoce difícil cumplimiento ENS de forma individualizada, por sus especiales características. Necesidad de mecanismos de adecuación e implantación multi-organismo para certificación de forma optimizada.

4. ASISTENCIA DIPUTACIONES A AYUNTAMIENTOS

APLICACIÓN ENS Y RGPD+LOPDGDD EN PEQUEÑOS AYUNTAMIENTOS

CCN: ITINERARIO DE ACCIONES DEL MARCO CERTIFICACIÓN ENS PARA EELL



4. ASISTENCIA DIPUTACIONES A AYUNTAMIENTOS

APLICACIÓN ENS Y RGPD+LOPDGDD EN PEQUEÑOS AYUNTAMIENTOS

DPD+RSEG

- Política seguridad y privacidad. Inexistencia de conflicto de intereses.
- Separación de tareas asesoramiento y control, de operativa seguridad.
- Aplicación de controles principalmente fuera ámbito Ayuntamiento.
- Responsable de Seguridad (RSEG)
 - Cumplimiento política de seguridad [y privacidad].
 - Aplicación del ENS. Declaración de aplicabilidad. Auditorias.
- Delegado de Protección de Datos (DPD)
 - Protección derechos y libertades ciudadano@s tratamiento datos.
 - Aplicación arts. 28 y 32 y RD 14/2019 en el proveedor de servicios.
 - Vigilancia utilización NNTT: Blockchain, BD, IA. Realización EIPD.

4. ASISTENCIA DIPUTACIONES A AYUNTAMIENTOS

APLICACIÓN ENS Y RGPD+LOPDGDD EN PEQUEÑOS AYUNTAMIENTOS

AEPD: HITOS PRINCIPALES ADECUACIÓN AAPP AL RGPD+LOPDGDD

1. Designación Delegado de Protección de Datos (DPD).
2. Elaboración Registro Actividades de Tratamiento (RAT).
3. Analizar bases jurídicas de los tratamientos.
4. Análisis de Riesgos e implantación medidas de seguridad.
5. Verificación medidas seguridad y notificación brechas seguridad.
6. Si procede, realización EIPD.
7. Redacción cláusulas informativas para recogida datos personales.
8. Establecer procedimientos para facilitar ejercicio de derechos.
9. Establecer procedimientos recabar/revocar consentimientos.
10. Valorar ET ofrecen garantías suficientes y adaptar contratos.
11. Confeccionar e implantar Políticas de Protección de datos.
12. Elaborar y ejecutar plan de formación y concienciación del personal.

4. ASISTENCIA DIPUTACIONES A AYUNTAMIENTOS

APLICACIÓN ENS Y RGPD+LOPDGDD EN PEQUEÑOS AYUNTAMIENTOS

CCN: HITOS PRINCIPALES ADECUACIÓN AAPP AL ENS

1. Designación roles seguridad: RSEG, RSERV, RINF, RSIST.
2. Redacción Política de Seguridad.
3. Elaboración Normativa y Procedimientos de Seguridad.
4. Inventario de activos.
5. Categorización del Sistema.
6. Análisis de Riesgos y tratamiento.
7. Declaración de aplicabilidad.
8. Configuración de las medidas de seguridad.
9. Gestión y Registro de Incidentes de Seguridad.
10. Contrataciones y acuerdos de nivel de servicio.
11. Concienciación y formación del personal.
12. Plan de Mejora de la seguridad (PDCA).

4. ASISTENCIA DIPUTACIONES A AYUNTAMIENTOS

APLICACIÓN ENS Y RGPD+LOPDGDD EN PEQUEÑOS AYUNTAMIENTOS

SIMBIOSIS APLICACIÓN ENS+RGPD+LOPDGDD EN PEQUEÑOS AYUNTAMIENTOS

- Tareas proactivas (vinc. PDCA) y reactivas (p.ej. Brechas de seguridad).
- Orientación al riesgo: Sistemas de Gestión de Seguridad y Privacidad.
- Auditorías conjuntas ENS y RGPD+LOPDGDD: optimización recursos.
- Aprobación de un Política [conjunta] de Seguridad y Privacidad.
- Análisis de Riesgos: diferentes vertientes pero herramientas conjuntas.
- RAT y Catálogo de Procedimientos Administrativos Sede Electrónica.
- Inventario de Sistemas Información utilizados.
- Revisión cláusulas contrataciones y alerta con brechas de seguridad.
- Formalización del procedimiento tratamiento brechas de seguridad.
- Concienciación, información y formación del personal: factor humano.
- RESULTADO: Mejora en la gestión administrativa del Ayuntamiento.

5. ASPECTOS SOBRE LA TECNOLOGÍA CLOUD

SERVICIOS CLOUD EN LAS ADMINISTRACIONES PÚBLICAS

FACTORES PROPICIAN INCREMENTO UTILIZACIÓN SERVICIOS EN LA NUBE.

- Redes alta velocidad y baja latencia: menor precio y mayor cobertura.
- Virtualización de servidores corporativos.
- Reducciones del coste de provisión y explotación de servicios.

FACTORES REQUIEREN ESPECIAL ATENCIÓN EN LA MIGRACIÓN A LA NUBE

- Refuerzo de los acuerdos de nivel de servicio en contrataciones.
- Condiciones legales ET servicios cloud: art. 28 RGPD y RD 14/2019.
- Criticidad de aspectos de seguridad y disponibilidad de las soluciones.
- Posibilidad de separación de RSEG y DPD en AAPP mayor tamaño.
- Aprovechamiento de las sinergias entre ENS y RGPD+LOPDGDD.
- Posibles criterios de solvencia y de valoración para servicios *cloud*.

5. ASPECTOS SOBRE LA TECNOLOGÍA CLOUD

SELECCIÓN DE ET Y GARANTÍAS APLICACIÓN MEDIDAS APROPIADAS.

NORMATIVAS DE APLICACIÓN.

- ENS: Misma categoría que AP contratante, pero recomendable ALTO.
- Certificaciones acreditativas de garantías suficientes para servicio:
 - Certificación de Gestión de servicios de TI.
 - Certificación de Sistema Gestión de Seguridad.
 - Certificación de controles adicionales sobre privacidad.
 - Certificación de controles de seguridad para servicios *cloud*.
 - Código de buenas prácticas protección datos personales en *cloud*.
 - Certificaciones de continuidad de negocio/servicio.
- Cumplimiento de legislación NIS (RDL 12/2018, de 7 de septiembre, y RD desarrollo 43/2021, de 26 de enero, que trasponen la Directiva UE 2016/1148, de 6 de julio, conocida como Directiva NIS) aplicable a servicios de computación en la nube.

5. ASPECTOS SOBRE LA TECNOLOGÍA CLOUD

EFFECTOS DEL ALEJAMIENTO DE LOS SERVICIOS TIC EN LAS AAPP.

¿QUÉ EFECTOS PRODUCIRÁ LA MIGRACIÓN DE SERVICIOS TIC AL CLOUD?.

- Administración como prescriptor de medidas técnicas y organizativas.
- Importancia de las TIC “locales” en función categoría de servicio *cloud*.

IaaS – PaaS – SaaS
+TIC -TIC

- Soporte TIC “local”: como mínimo soporte a los puestos de trabajo.
- Prestar especial atención a:
 - condiciones de portabilidad en el *cloud*.
 - “cliente cautivo”.
 - De nuevo normativa: ENI (RD 4/2010, 8 de enero y NN TT).

6.CONCLUSIONES

CONCLUSIONES

LEGISLACIÓN DE OBLIGADO CUMPLIMIENTO POR AAPP DE TODOS TAMAÑOS

- Esquema Nacional de Seguridad.
- Reglamento General de Protección de Datos.
- Ley Orgánica de Protección de Datos y Garantía Derechos Digitales.

PROPUESTA APLICACIÓN CONCURRENTE EN PEQUEÑOS AYUNTAMIENTOS

- DPD + RSEG @ Diputación, garantizando independencia funciones.
- Solución debe ser: sencilla, escalable y sostenible en el tiempo.
- Ofrecer todas las garantías de seguridad técnica y jurídica.

RESULTADO DE LA APLICACIÓN DE LA PROPUESTA

- Mejora en la gestión, prestación servicios, seguridad y privacidad.
- Impulso a la transformación digital y modernización administrativa.



Diputación
de Salamanca



CIPSA
ORGANISMO AUTÓNOMO
CENTRO INFORMÁTICO PROVINCIAL
S A L A M A N C A

MUCHAS GRACIAS