

# XII Jornadas STIC CCN-CERT

Ciberseguridad,  
hacia una respuesta y disuasión efectivas



Al final del camino está la  
recompensa. Certificación  
del Esquema Nacional de  
Seguridad en el primer  
Ayuntamiento de España



- Miguel A. Lubián
- Grupo CIES (Instituto CIES y AliSEC)
- [miguel.Lubian@institutocies.es](mailto:miguel.Lubian@institutocies.es)



**ALFONSO DOU OBLANCA**

Ingeniero informático por la Universidad de Oviedo.

**Jefe de Sección de Nuevas Tecnologías.**  
en el Ayuntamiento de Avilés



**Delgado, Boris**

Gerente de Certificación TIC

**AENOR**



# Índice

1. Enfoque metodológico. - es +
2. Certificación: ¿Qué ha pasado durante este último año? ¿Por qué?
3. Making Of en el Ayuntamiento de Avilés
4. Conclusiones





## Enfoque Metodológico

- Las AAPP, y sobre todo en Entidades Locales, tienen **dificultades para “asimilar nuevas figuras”**, que vienen implícitas en el ENS y RGPD, **así como asumir responsabilidades.**

(Próximamente: Revisión de la guía CCN-STIC-801 sobre Responsabilidades)

- **Las Administraciones necesitan ENS para cumplir RGPD**, es decir, necesitan proteger sus datos con algo más que cláusulas.

(Nueva guía CCN-STIC 881 Impacto RGPD en ENS)

- Los **caminos** para llegar al cumplimiento **no son únicos** (RD 951/2015 artículo 27, apartado 5)

(Nueva guía CCN-STIC 819 sobre Medidas Compensatorias)



# Índice

**1. Enfoque metodológico. - es +**

2. Certificación: ¿Qué ha pasado durante este último año? ¿Por qué?

3. Making Of en el Ayuntamiento de Avilés

4. Conclusiones



# XI JORNADAS STIC CCN-CERT

Ciberamenazas\_  
El reto de compartir

#XIJornadasCCNCERT

MADRID.  
13 Y 14 DE DICIEMBRE  
2017

"La aplicación el Esquema Nacional de Seguridad en las Administraciones  
Públicas bajo un enfoque práctico"

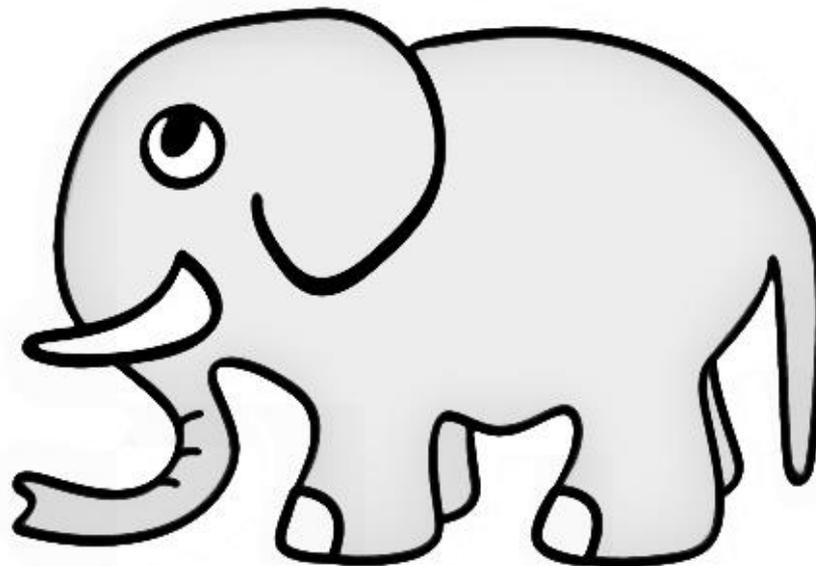
## Menos es Más

- ES +



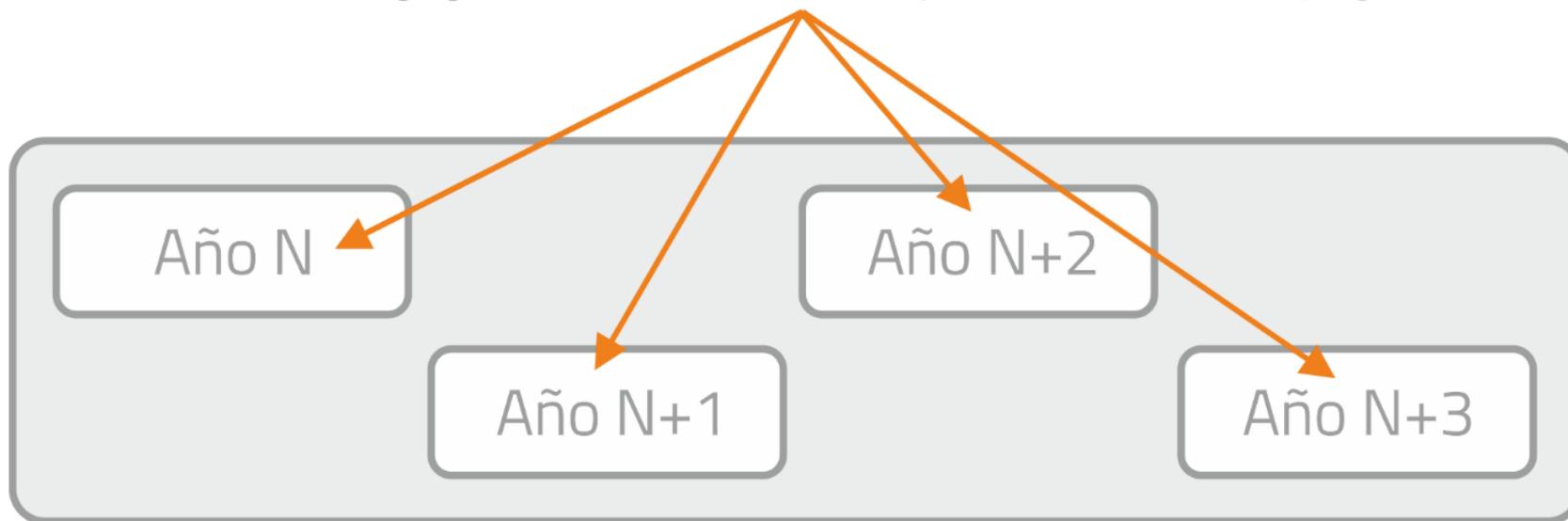


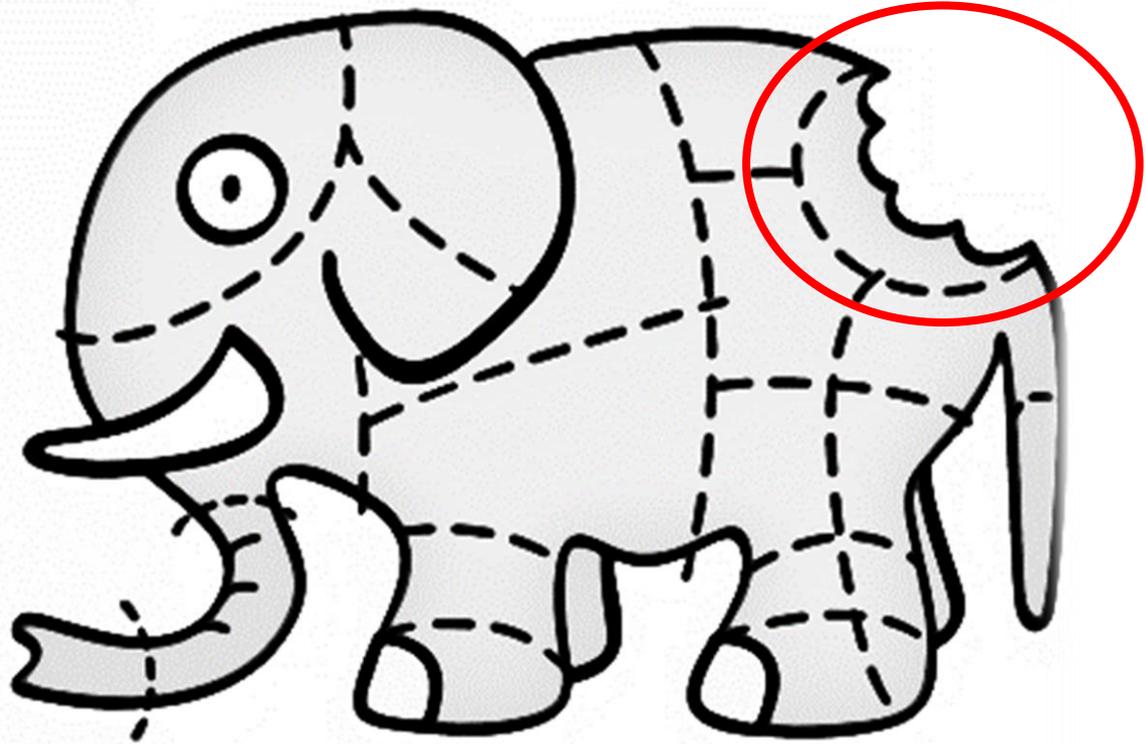
Vimos que teníamos un reto.  
Definir la estrategia para...



- ES +

PRIMERA PROPUESTA Segregar en diferentes subsistemas y buscar la **conformidad progresiva en el tiempo**.





Hoy, un año después, veremos las **primeras consecuencias** de aplicar este “enfoque progresivo” (**Posibilista**)

**El resultado de su aplicación: Hemos conseguido el 25% aproximadamente de las certificaciones actuales**



# Índice

1. Enfoque metodológico. - es +

**2. Certificación: ¿Qué ha pasado durante este último año? ¿Por qué?**

3. Making Of en el Ayuntamiento de Avilés

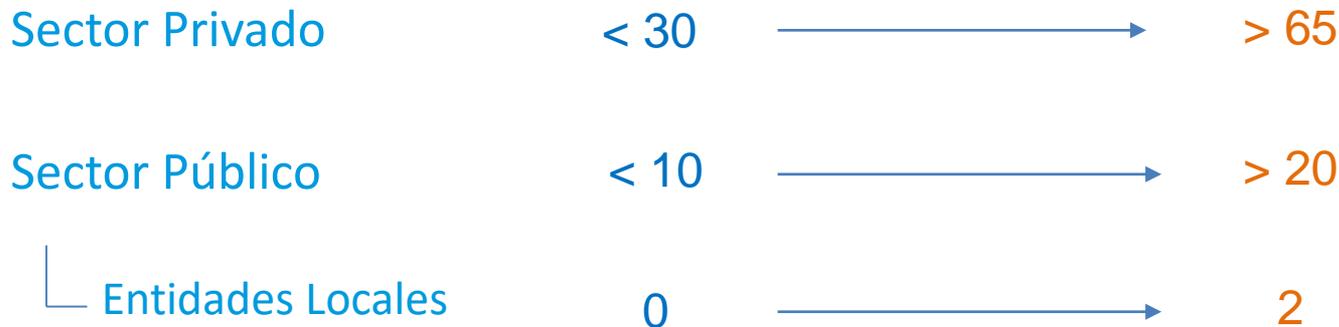
4. Conclusiones



## Evolución de la Conformidad

Evolución de la conformidad

2015..2017                      2018



¿A qué debemos este notable incremento en el sector privado?

¿Por qué empiezan a despertar los primeros Ayuntamientos?



## Las empresas privadas

Se están encontrando la “obligación” de implementar medidas de seguridad conforme al ENS consecuencia de los pliegos de contratación.

La proporcionalidad en los pliegos se agota ...

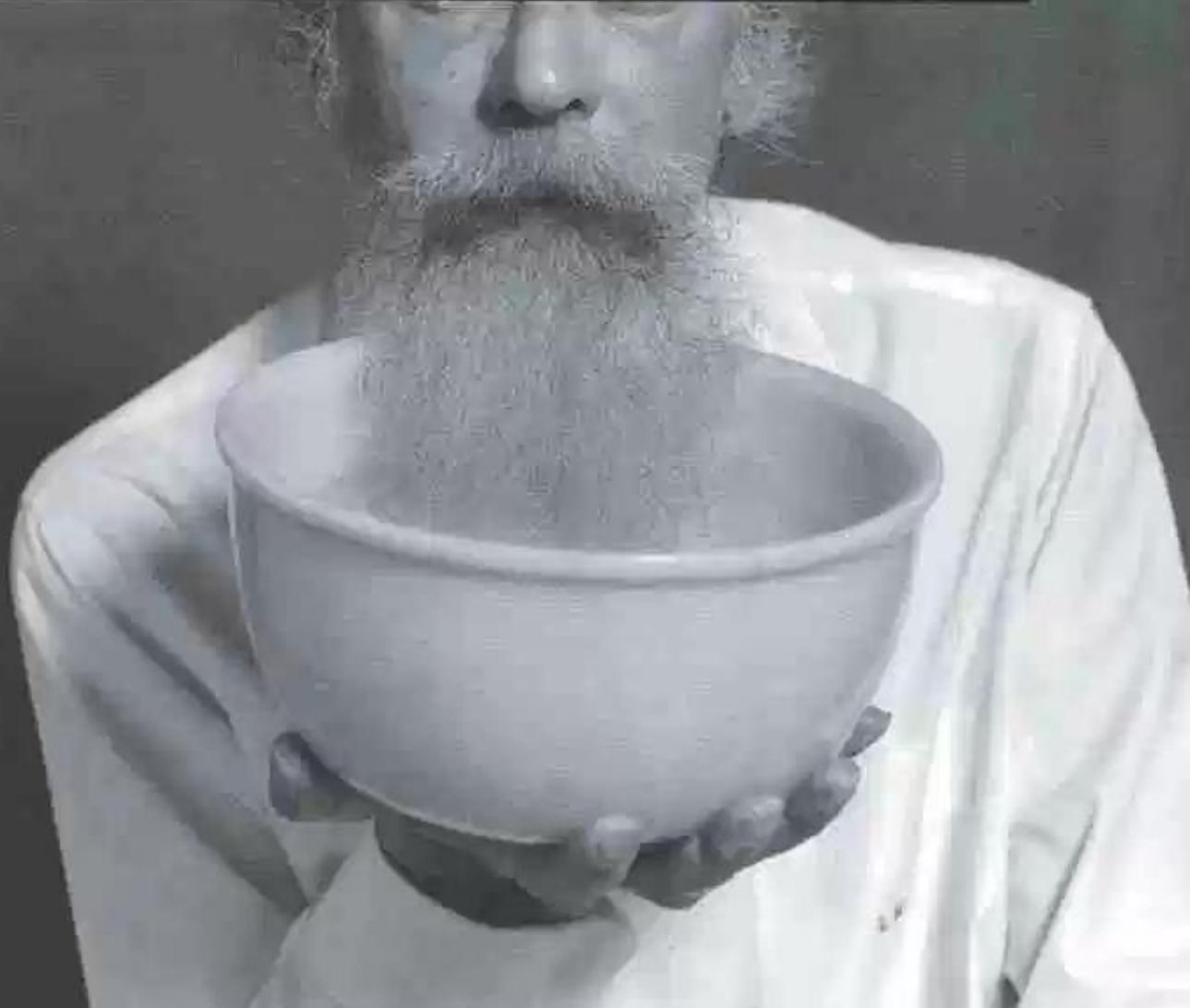




## Las Administraciones

Saben que no tener ENS genera una inseguridad jurídica en la tramitación electrónica (Leyes 39 y 40/2015, Ley 9/2017 LCSP, etc.)

Y, simplemente, empiezan a ver necesario implementar seguridad, es decir buscar conformidad con el ENS



Quando las barbas  
de tu vecino veas  
cortar ...



# Índice

1. Enfoque metodológico. - es +
2. Certificación: ¿Qué ha pasado durante este último año? ¿Por qué?
- 3. Making Of en el Ayuntamiento de Avilés**
4. Conclusiones

# CLAVES

1

Enfocar correctamente el proyecto  
dentro de la entidad



Todas las personas implicadas en el proceso deben conocer, en la medida que les resulte de aplicación, los principales riesgos.

Así comprenderán por qué aplicamos algunas determinadas medidas de seguridad



**CTRL + C**

**CTRL + V**

No se trata de generar un **PACK de documentación**, sino de proteger los sistemas de información, aplicando medidas de seguridad.



# Recuerda

Estas teclas no funcionan cuando se produce un incidente de seguridad.



Seguridad Perimetral	Firewall	WAF	Antispam	Proxy	Balanceadores	VPN	Aceleradores WAN	DoS/DDoS
Seguridad Red	IDS	NAC	Segmentación	IPAM	Monitorización	Bridge	WiFi	SIEM
Seguridad Puesto	Antivirus	HIDS	MDM	Gestión Identidades	DLP	IRM	Backup	Inventario
Seguridad Física	Control Accesos	Videovigilancia	Extinción	Climatización	Cableado	Alimentación	Suelo/Techo Técnico	Redundancia

¿Cuántas tenemos aplicadas?





Miguel, muchas de estas medidas no están  
en el Anexo II del RD 3/2010...  
(Principios básicos y requisitos mínimos)



**!! No sólo hay que aplicar las medidas de seguridad que tenemos en el Anexo II del RD 3/2010 !!**

Tendrías que aplicar, **adicionalmente**, las **medidas de seguridad resultantes (necesarias) de tu análisis del riesgo.**

En RGPD lo alinearemos con PdD y con el principio de responsabilidad activa (Accountability)



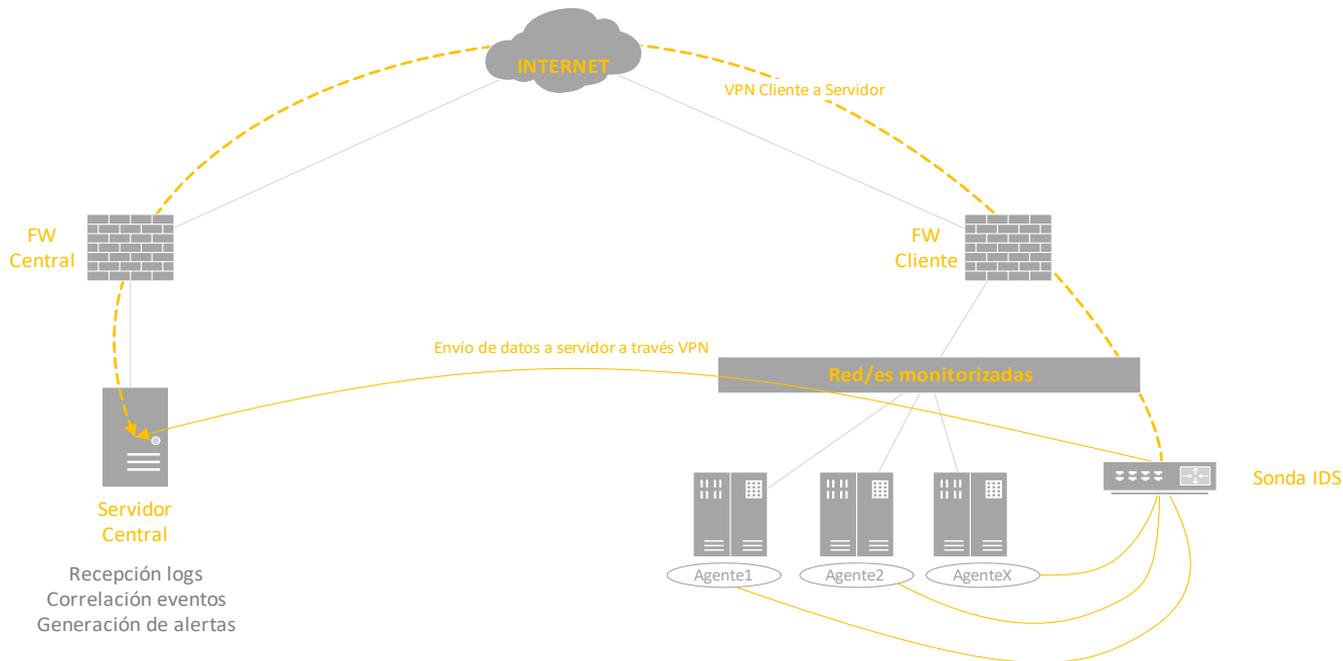
¿Cómo vas a gestionar tus brechas de seguridad?

¿Cómo vas a garantizar la trazabilidad de los usuarios?





# Es fundamental, Monitorizar los sistemas, la correlación de eventos (SIEM) y su correspondiente revisión de registros





Y poco a poco se acercará el temido día...



Nombre	Razón social	Enlace web	Estado Acreditación ENS
AENOR Internacional S.A.U.	AENOR Internacional S.A.U.	<a href="http://www.aenor.com">www.aenor.com</a>	ACREDITADA (21/04/2017)
Audertis Audit Services, S.L.	Audertis Audit Services, S.L.	<a href="http://www.audertis.es">www.audertis.es</a>	ACREDITADA (29/12/2017)
BDO Auditores, S.L.P.	BDO Auditores, S.L.P.	<a href="http://www.bdo.es">www.bdo.es</a>	ACREDITADA (15/06/2018)
Cámara Certifica	Certificación y Confianza, Cámara S.L.U.	<a href="http://camaracertifica.es/">camaracertifica.es/</a>	EN PROCESO (DESDE 27/10/2017)
Eurocertificación	Eurocert Certification Spain S.L.	Desconocida	EN PROCESO (DESDE 27/10/2017)

...



# El auditor no es el rival ... Tus enemigos son otros





Ni tampoco tiene una función  
de inspector....



```

/**
 * Handles XML content
 */
public class XStreamHandler implements ContentTypeHandler {

    public String fromObject(Object obj, String resultCode, Writer out) throws IOException {

        if (obj != null) {
            XStream xstream = createXStream();
            xstream.toXML(obj, out);
        }
        return null;
    }

    public void toObject(Reader in, Object target) {
        XStream xstream = createXStream();
        xstream.fromXML(in, target);
    }

    protected XStream createXStream() {

        return new XStream();
    }
}

```

```

/**
 * Handles XML content
 */
public class XStreamHandler extends AbstractContentTypeHandler {

    private static final Logger LOG = LogManager.getLogger(XStreamHandler.class);

    public String fromObject(ActionInvocation invocation, Object obj, String resultCode, Writer out) throws IOException {
        if (obj != null) {
            XStream xstream = createXStream(invocation);
            xstream.toXML(obj, out);
        }
        return null;
    }

    public void toObject(ActionInvocation invocation, Reader in, Object target) {
        XStream xstream = createXStream(invocation);
        xstream.fromXML(in, target);
    }

    /**
     * @deprecated use version with {@link ActionInvocation}
     */
    @Deprecated
    protected XStream createXStream() {
        LOG.warn("You are using a deprecated API!");
        return new XStream();
    }
}

```



¿ Podrías engañarlo?



Te engañarías a ti mismo....



Tu objetivo es  
**dormir tranquilo**

# Sleeping Positions



**CEO**



**CFO**



**COO**



**CISO**

# CLAVES

2

Definición de un alcance posibilista  
(Año 1)

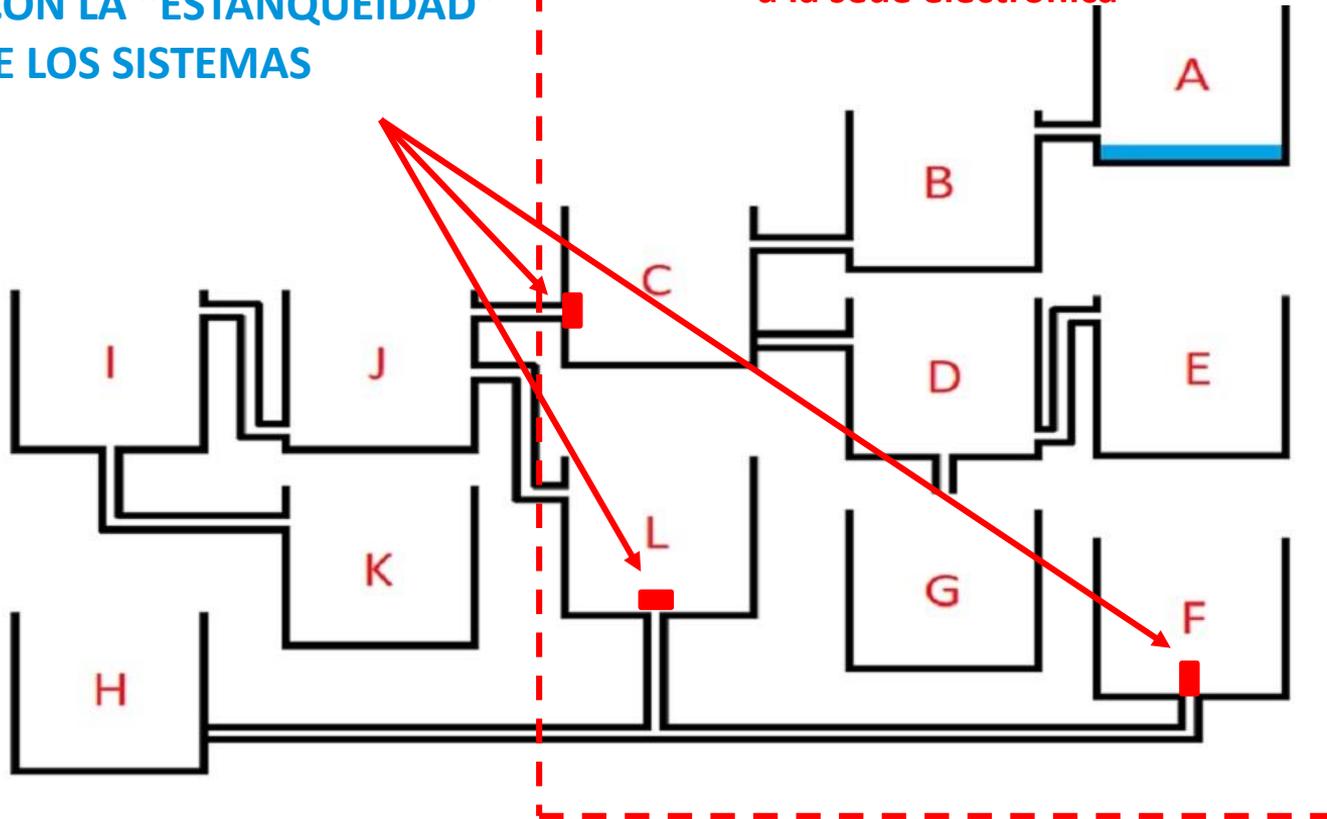
SI ESTOS FUESEN TODOS TUS SISTEMAS DE  
INFORMACION ...



**CUIDADO CON LA “ESTANQUEIDAD”  
DE LOS SISTEMAS**

**ALCANCE AÑO 1**

**Sistemas de información que dan soporte  
a la sede electrónica**



# CLAVES

3

Comenzamos a implantar las  
medidas de seguridad  
(Anexo II + Derivadas del Análisis del Riesgo)

## Organización de la Seguridad [org.1]



¿Contamos con nuestros políticos?  
¿Para que os sirve el Comité de Seguridad?  
¿Ha sido difícil crearlo?



¿Pasamos sin Delegado de Protección de Datos?  
¿Se puede externalizar el Responsable de Seguridad?

## Normativa de seguridad [org.2] y [mp.per2, mp.per3 y mp.per4]



¿Cómo gestionamos este proceso?

¿Cómo acreditar su lectura y comprensión?

¿Cómo se conecta con el RGPD?

## ¿Cómo hemos evidenciado la implantación de medidas?



¿Qué Herramienta utilizamos?

¿Ha sido importante durante el proceso de auditoría?

¿Cómo gestionamos las altas y bajas de los usuarios?

## ¿Cómo intentamos dormir tranquilos?

¿Hacking ético? ¿Salieron cosas?



¿IDS Red? ¿Host? ¿SIEM? ¿Tenemos tiempo para revisar?

¿Doble barrera perimetral? ¿Aunque estemos en categoría media?

¿Ingeniería social, NAC, auditorías en puntos de impresión, auditorías de aplicaciones...? ¿Presente y futuro?

## ¿Cómo lo afrontamos [op.acc.5]?



## ¿Cómo lo afrontamos [op.acc.5]?



Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen, pudiendo usarse los siguientes factores de autenticación:

- "algo que se sabe": contraseñas o claves concertadas.
- "algo que se tiene": componentes lógicos o dispositivos físicos
- "algo que se es": elementos biométricos.

**QUE NO  
SALGA DE AQUÍ**



## Otras cosas que se analizarán...

1. Analizar si te resulta de aplicación otras normativas como PCI DSS (aunque sea pasarela externa.)
2. Si aparecen tus terceros en PILAR...
3. Revisión de terceros (SLA, RGPD, Revisión del alcance en la conformidad ENS...)
4. Sistemas operativos y equipamiento fuera de soporte.
5. Caídas de @firma registradas en tu gestor de incidencias.
6. Indicadores de cumplimiento y frecuencias de actualización (CCN-STIC 844)
7. Conocer exactamente los protocolos de cifrado que usan los sistemas.
8. Revisión y comprobación sobre el inventario de activos.
9. Copias de seguridad (inclusive de la configuración de los Firewall)
10. Gestión de incidentes de seguridad. Ver tipificación guía CCN-STIC 817. Alineamiento con LUCIA.
11. Gestión de certificados electrónicos.

## Otras cosas que se analizarán...

1. Verificación de los accesos remotos (VPN)
2. Configuración de directivas (No sólo GPO de DA. Políticas en sistemas Linux, SGBD).  
Herramienta de verificación CLARA.
3. Cumplimiento RGPD. Alineamiento del AARR.
4. Instrucciones técnicas de bastionado. Herramienta ROCIO.
5. Procedimiento de altas y bajas. Precaución si somos CA con las bajas de los certificados electrónicos.
6. Control de discos duros en caso de avería con el fabricante. (Guía CCN-STIC 305)
7. Firma electrónica. Revisión de algoritmos no permitidos.
8. Gestión de Metadatos (Verificación de documentos aleatorios)
9. Utilización de metodologías de desarrollo seguro. Conocimiento de pruebas realizadas por tus prestadores.
10. Visita al CPD: Inspección de industria, revisión del informe de incendios, bombas de achique

# CLAVES

4 La recompensa es parte del proceso

# Certificado de Conformidad con el Esquema Nacional de Seguridad



**ENS-2018/0010**

AENOR, certifica que los sistemas de información reseñados todos ellos de categoría MEDIA, y los servicios que se relacionan, de:

## AYUNTAMIENTO DE AVILÉS

han sido auditados y encontrados conforme con las exigencias del Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, según se indica en el correspondiente Informe de Auditoría de 2018/06/25

para: Los sistemas de información que dan soporte a la Sede electrónica del Ayuntamiento de Avilés de acuerdo con la categorización del sistema vigente.

que se realizan: PL DE ESPAÑA, 1.33400 - AVILÉS (ASTURIAS)

Fecha de certificación de conformidad inicial: 2018-07-20  
Fecha de renovación certificación de conformidad: 2020-07-20  
Número de certificado: ENS-2018/0010

Fecha: Madrid 20 de Julio de 2018



Rafael GARCÍA MEIRO  
Director General

Los sistemas de información que dan soporte a la Sede electrónica del Ayuntamiento de Avilés de acuerdo con la categorización del sistema vigente.





Es el mejor premio para tu equipo de trabajo.

**Avilés, ha sido el primer Ayuntamiento de España en tener conformidad con el ENS**

# CLAVES

## 5

Claves y lecciones aprendidas  
(Alfonso Dou. Ayuntamiento de Avilés)



## Ayuntamiento de Avilés

Claves y lecciones aprendidas

- ¿Podemos dejar a los políticos al margen? **No**
- ¿Medidas de seguridad clave? **Monitorización y sensibilización**
- ¿Cómo lo evidenciamos? **Herramienta con flujos probación**

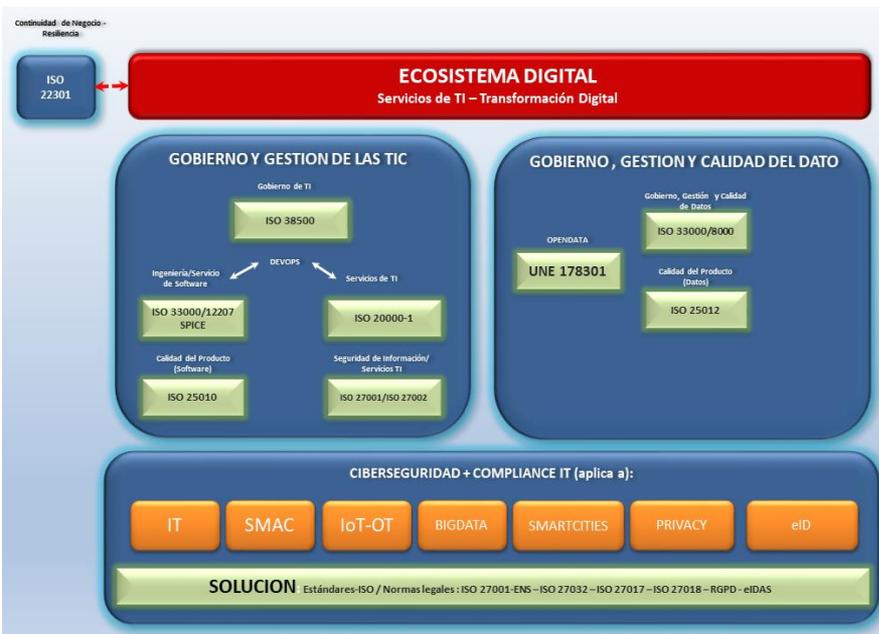
¿Qué ha supuesto el ENS para vuestro trabajo?  
¿Recomendable?

# CLAVES

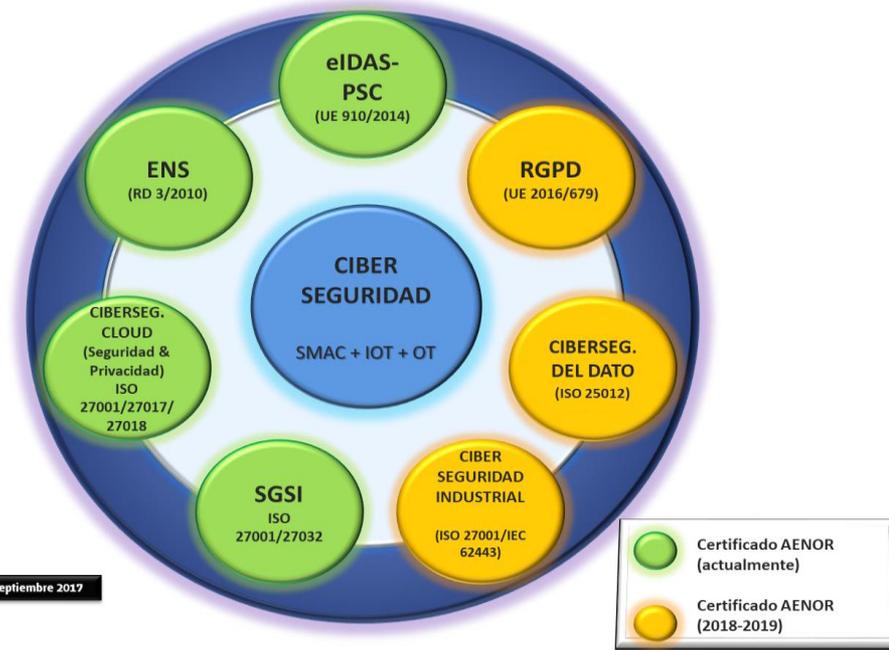
6

El Ecosistema Digital  
(Boris Delgado. Aenor)

# 1. ECOSISTEMA DIGITAL DE AENOR. TRES MODELOS INTERRELACIONADOS



Fuente: Carlos Manuel Fdez. y Boris Delgado  
 VIDEO AENOR: [https://youtu.be/ZSLf7l\\_OYS0](https://youtu.be/ZSLf7l_OYS0)



Fuente: AENOR-TIC: Septiembre 2017

[www.aenor.com/certificacion/tecnologias-de-la-informacion](http://www.aenor.com/certificacion/tecnologias-de-la-informacion)  
[www.aenorciberseguridad.com/](http://www.aenorciberseguridad.com/)



# Índice

1. Enfoque metodológico. - es +
2. Certificación: ¿Qué ha pasado durante este último año? ¿Por qué?
3. Making Of en el Ayuntamiento de Avilés
4. Conclusiones

Ninguna consultora te podrá vender el ENS como un producto paquetizado, ni existen herramientas mágicas para hacer ENS. Se trata de un proceso interno, en el que puedes tener acompañamiento y servicios.





**“Estudia, no empolles”**

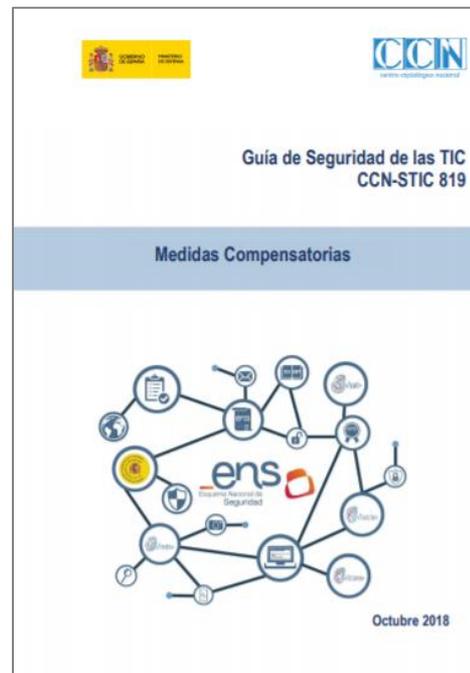
¿Podrías tener conformidad sin mejorar la seguridad?

**Centra mejor tus esfuerzos en mejorar**





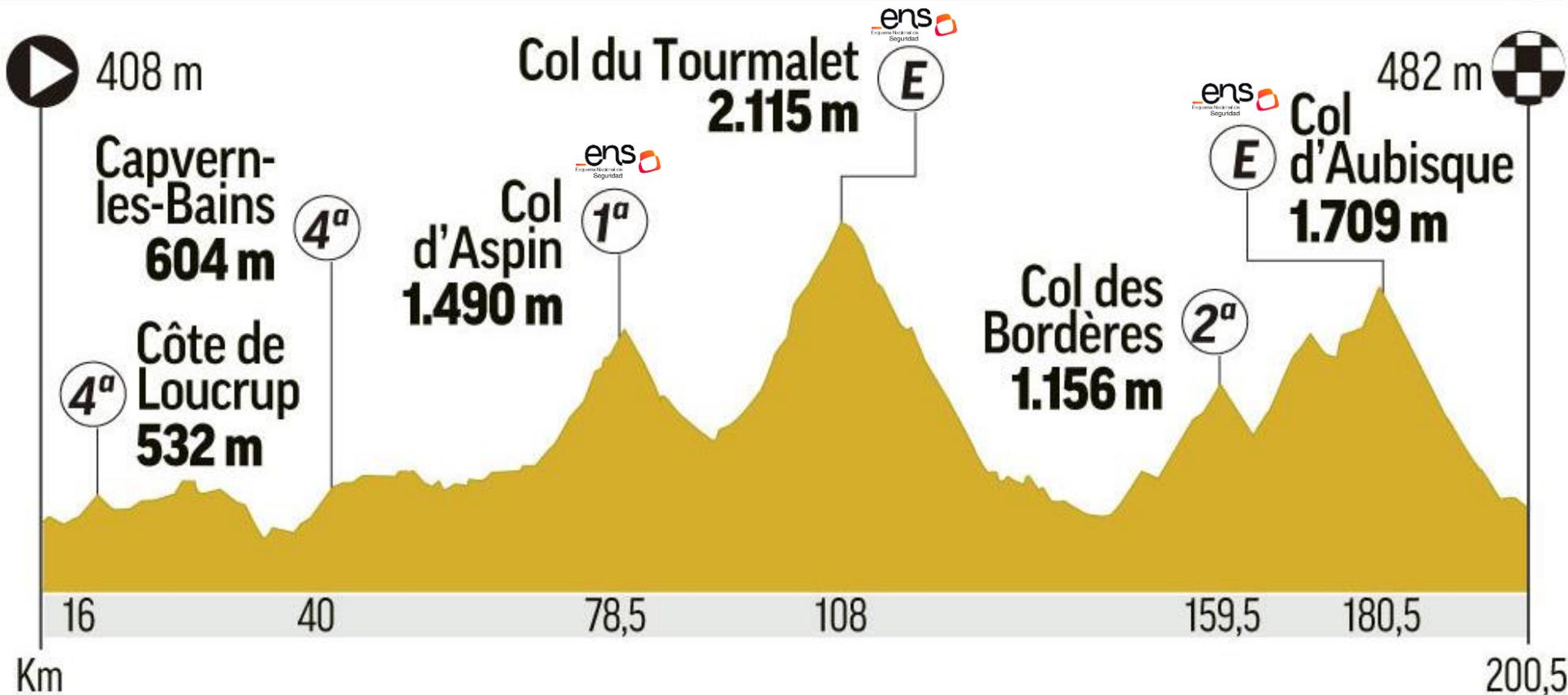
Los caminos para llegar al cumplimiento no son únicos (Guía CCN-STIC 819)





# MONITORIZA. ESTA NO ES LA SOLUCIÓN







Tus políticos /directivos deben saber entender la seguridad como un proceso continuado, y no como un proyecto puntual.

Necesitas tiempo, recursos y presupuesto.

One more thing...



# XII Jornadas STIC CCN-CERT

Ciberseguridad,

hacia una respuesta y disuasión efectivas



## ▶ E-Mails

- ▶ [info@ccn-cert.cni.es](mailto:info@ccn-cert.cni.es)
- ▶ [ccn@cni.es](mailto:ccn@cni.es)
- ▶ [organismo.certificacion@cni.es](mailto:organismo.certificacion@cni.es)

## Websites

- ▶ [www.ccn.cni.es](http://www.ccn.cni.es)
- ▶ [www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)
- ▶ [oc.ccn.cni.es](http://oc.ccn.cni.es)

## ▶ Síguenos en

