



XIII JORNADAS STIC CCN-CERT



LA CERTIFICACIÓN DE PERSONAS

Una herramienta eficaz
para facilitar la implementación efectiva
del ENS en las Entidades Públicas
y sus Proveedores

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT



Miguel Angel Vila Espeso

IVAC – INSTITUTO DE CERTIFICACIÓN

ivac@ivac.es

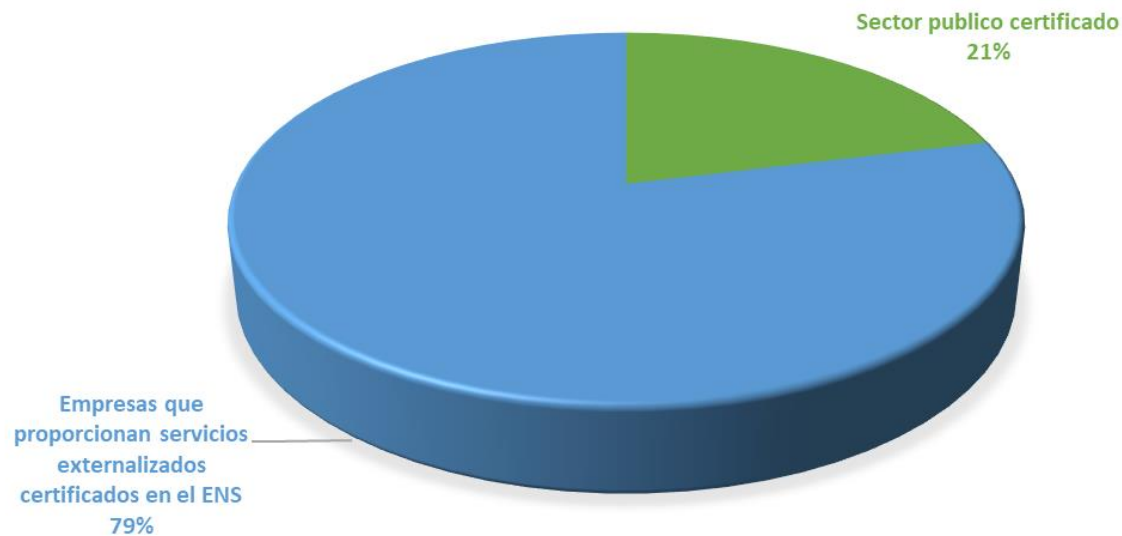
Índice

1. Hacia la implementación efectiva del ENS
2. La Certificación de Personas
3. El Esquema de Certificación de Personas. La norma ISO 17024
4. La Certificación de Personas en el ámbito del ENS:
El Responsable de Seguridad
5. El Responsable de la Seguridad y de la Privacidad
6. Conclusiones

1. HACIA LA IMPLEMENTACION EFECTIVA DEL ENS

SITUACIÓN ACTUAL

- 38 Entidades Certificadas del Sector Público
- 141 Empresas que proporcionan servicios externalizados certificados en el ENS



Fuente CCN-CERT (14-Nov-2019)

1. HACIA LA IMPLEMENTACION EFECTIVA DEL ENS

Retos a los que se enfrentan las Entidades Públicas y las Empresas

- CONCIENCIACIÓN RESPONSABLES POLÍTICOS – NECESIDAD
- RECURSOS ECONÓMICOS
 - Renovación equipos informáticos; Adaptación de los existentes a las nuevas exigencias de configuración
- RECURSOS HUMANOS
 - **Carencia muy importante de personal cualificado**
 - Entidades Públicas: ¿Qué debo licitar?
 - Empresas: ¿Quién me ayuda?
- CORPUS DOCUMENTAL: *Ingente y Prolijo*
- LA COMPETENCIA DEL RESPONSABLE DE SEGURIDAD
No solo en el área técnica



1. HACIA LA IMPLEMENTACION EFECTIVA DEL ENS

Retos a los que se enfrentan las Entidades Públicas y las Empresas

Uno de los retos (COMPETENCIA – RECURSOS HUMANOS) se puede abordar con

LA CERTIFICACIÓN DE PERSONAS



2. LA CERTIFICACIÓN DE PERSONAS

Integrada en nuestro entorno

- Antecedentes: Los Gremios
- Actividad de Evaluación de la Conformidad regulada en el ámbito de la UE
- Reglamento /CE) nº 765/2008: Ley de Industria de 1992
- «evaluación de la conformidad»: proceso por el que se demuestra si se cumplen los requisitos específicos relativos a

Un Producto



Un Proceso – Un Servicio - Un Sistema



Una Persona



Un Organismo



- El aumento progresivo de Entidades de Certificación refleja la demanda del mercado de herramientas que aporten confianza

2. LA CERTIFICACIÓN DE PERSONAS

¿Qué es?

- Reconocimiento de la competencia profesional frente a un estándar (esquema de certificación).
- Facilita la diligencia debida en la contratación de personal / contratación de servicios profesionales.
- Obliga a la actualización de conocimientos: re-certificación.
- Herramienta de autorregulación de profesiones que aumenta el nivel de exigencia dificultando el intrusismo y el fraude.

2. LA CERTIFICACIÓN DE PERSONAS

Qué ventajas nos aporta

Principios básicos de la UE: libre circulación de mercancías, capitales, empresas y PERSONAS (física/fronteras - CONOCIMIENTO).

- Exigencia / Valoración del mercado laboral.
- Favorece / Apoya la contratación / Selección de personal.
- Oportunidad de desarrollo profesional:
 - ¿Quién me puede ayudar?
- Desarrollo tecnológico constante y a un ritmo vertiginoso:
actualización constante para mantener la certificación.

2. LA CERTIFICACIÓN DE PERSONAS

Aplicación en Sectores Profesionales Regulados

- La Certificación de Personas en la INDUSTRIA
 - Instalaciones contra incendios
 - Instalaciones de gas

TITULACIÓN OFICIAL REGLADA = CERTIFICACIÓN DE PERSONAS

- La Certificación de Personas en la MEDICINA

VPC Validación
Periódica
de la
Colegiación

2. LA CERTIFICACIÓN DE PERSONAS

Aplicación en Sectores Profesionales No Regulados

- La Certificación de Personas en el ámbito de la CIBERSEGURIDAD



2. LA CERTIFICACIÓN DE PERSONAS

Aplicación en Sectores Profesionales “Semirregulados”

- La Certificación de Personas en el ámbito de la PRIVACIDAD



2. LA CERTIFICACIÓN DE PERSONAS

La Certificación de Personas en el ámbito del ENS

Estrategia Nacional de Ciberseguridad 2019

Línea de acción 5, Objetivo IV

5. Actualizar, o en su caso **desarrollar marcos de competencias en ciberseguridad**, que respondan a las necesidades del mercado laboral.
6. Identificar las necesidades de capacidades profesionales de ciberseguridad, fomentando la colaboración con las instituciones educativas y formativas impulsando la formación continua, la formación para el empleo y universitaria, **promoviendo sistemas de acreditación y certificación profesional**.
7. Impulsar la inclusión de perfiles profesionales de ciberseguridad en las relaciones de puestos de trabajo del sector público.
8. Detectar, fomentar y retener el talento en ciberseguridad.

2. LA CERTIFICACIÓN DE PERSONAS

La Certificación de Personas en el ámbito del ENS

Real Decreto 3/2010 (ENS)

Artículo 15.3 Las **Administraciones públicas exigirán, de manera objetiva y no discriminatoria**, que las organizaciones que les presten servicios de seguridad cuenten con **profesionales cualificados** y con unos niveles idóneos de gestión y madurez en los servicios prestados.

3. EL ESQUEMA DE CERTIFICACIÓN DE PERSONAS

LA NORMA UNE-EN ISO/IEC 17024:2012



International
Organization for
Standardization

La norma ISO 17024 establece los requisitos para el desarrollo de esquemas de certificación de personas

- El uso de un estándar de reconocimiento internacional garantiza:
 - Un proceso aceptado globalmente
 - La participación activa de los expertos apropiados
 - La representación equitativa de los intereses de las partes interesadas
 - La correcta alineación de la evaluación y los requisitos de competencia
 - La revaluación periódica del proceso de certificación

3. EL ESQUEMA DE CERTIFICACIÓN DE PERSONAS

EL CONTENIDO DEL ESQUEMA



El alcance de certificación



La descripción del trabajo



La competencia requerida



Las aptitudes



Los prerrequisitos



El código de conducta

3. EL ESQUEMA DE CERTIFICACIÓN DE PERSONAS

EL PROCESO DE CERTIFICACIÓN

Los criterios para la certificación inicial y la renovación de la certificación

Los métodos de evaluación de la certificación inicial y la renovación de la certificación

Los métodos y los criterios de vigilancia

Los criterios para suspender y retirar la certificación

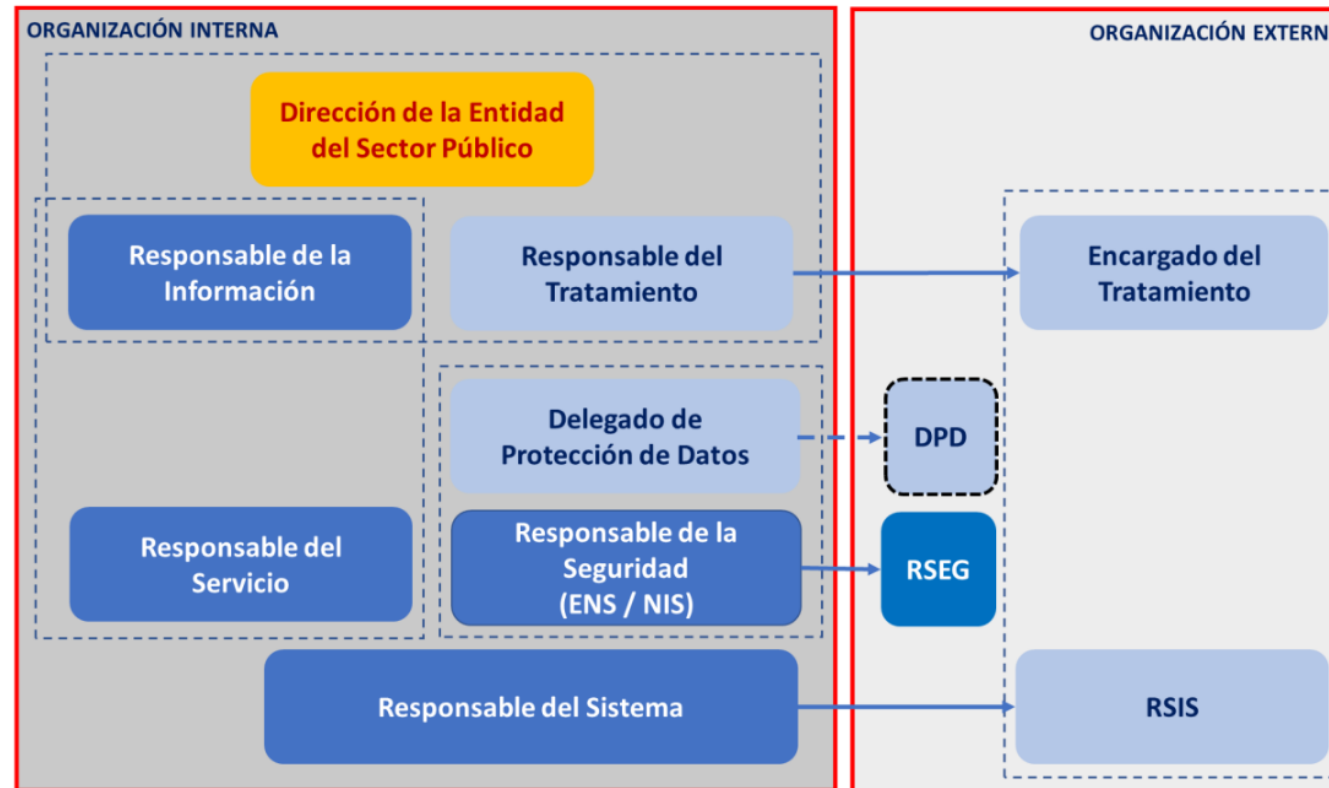
Los criterios para efectuar cambios en el alcance o en el nivel de la certificación

4. LA CERTIFICACION DE PERSONAS EN EL AMBITO DEL ENS

Actores y Responsables

CCN-STIC-801

Esquema Nacional de Seguridad – Responsabilidades



Esquema conceptual de la Seguridad de la Información y la Protección de Datos

4. LA CERTIFICACION DE PERSONAS EN EL AMBITO DEL ENS

El Responsable de Seguridad: Competencias y Funciones

Artículo 10 ENS

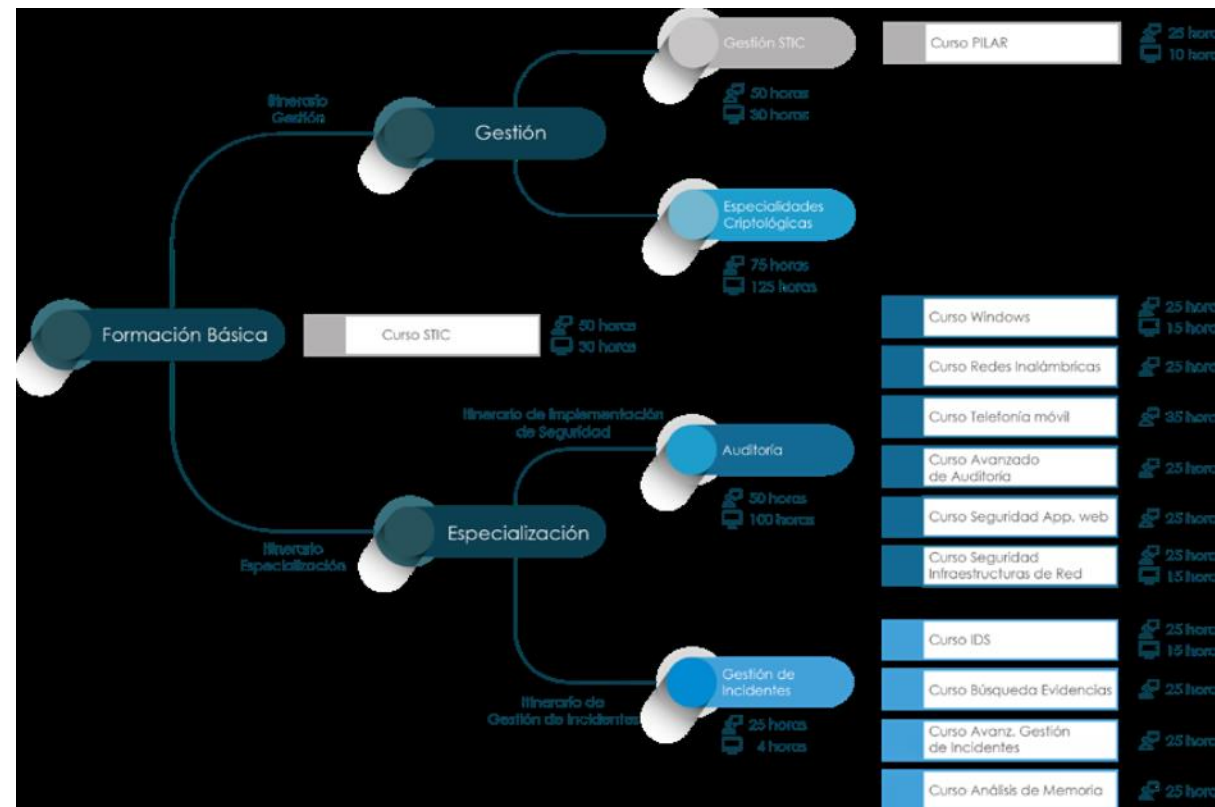
Funciones	“responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios”
Competencias	No establece competencias

CCN-STIC 801

Funciones	• “Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad de acuerdo con lo establecido en su política de seguridad de la información • “Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad”
Competencias	No establece competencias

4. LA CERTIFICACION DE PERSONAS EN EL AMBITO DEL ENS

El Responsable de Seguridad: Competencias



4. LA CERTIFICACION DE PERSONAS EN EL AMBITO DEL ENS

El Responsable de Seguridad: Competencias y Funciones

Funciones concretas y Competencias relacionadas

FUNCIONES	COMPETENCIAS	
Elaborar las políticas de seguridad Recibir, interpretar y supervisar la aplicación de instrucciones Suministrar información	TIC (sistemas de información, redes informáticas, entornos y sistemas operativos, virtualización de infraestructuras) Trabajar con modelos de sistemas	Capacidad de expresión escrita Sistemático STIC`s-CCN Habilidades directivas
Desarrollar las políticas de seguridad, normativas y procedimientos	TIC Capacidad de expresión escrita Sistemático	Análisis de riesgos: metodologías específicas STIC's-CCN Habilidades directivas
Supervisar las políticas de seguridad (supervisar su efectividad y llevar a cabo las auditorías periódicas)	TIC	Metodología de auditorías Habilidades sociales
Elaborar el documento de aplicabilidad de medidas de seguridad	STIC's-CCN	Capacidad de expresión escrita
Capacitador (formador)	Capacidades docentes	
Notificaciones de incidentes	TIC Análisis de problemas	Informática forense Informes escritos

4. LA CERTIFICACION DE PERSONAS EN EL AMBITO DEL ENS

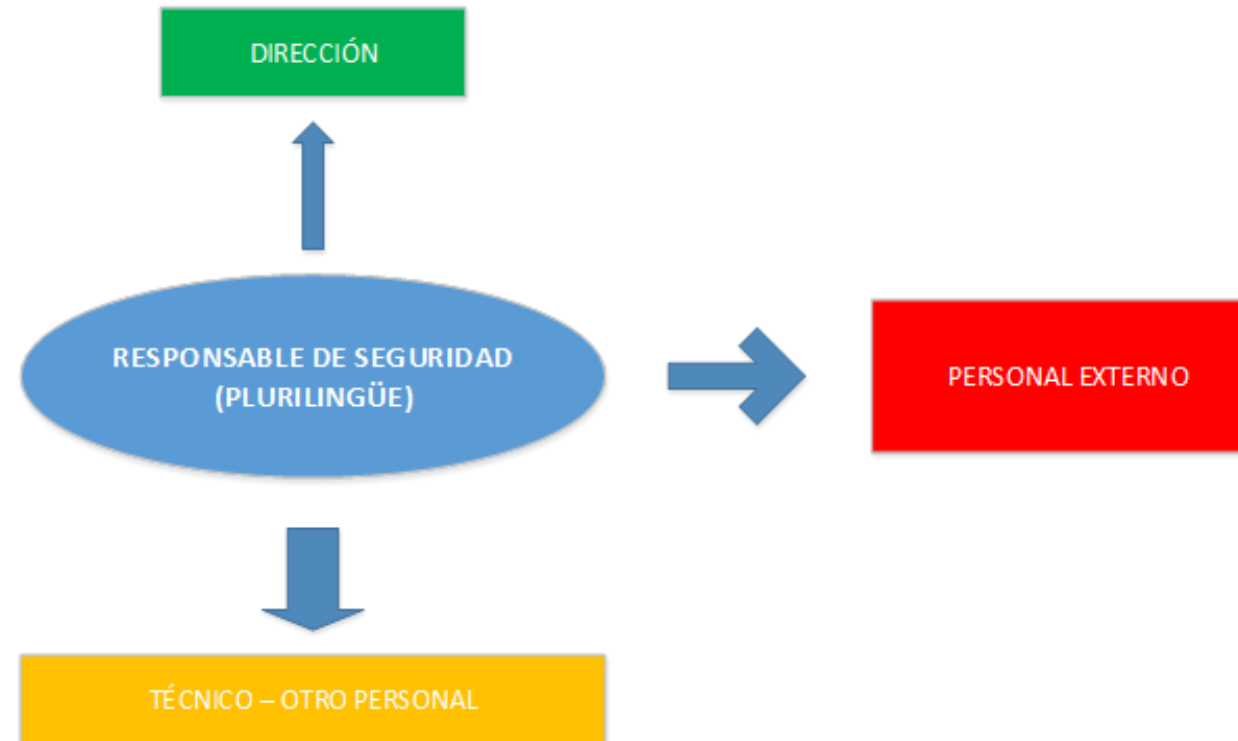
El Responsable de Seguridad: Competencias

Relación de Guías STIC que requieren un conocimiento “alto”

Serie STIC	Guía STIC
100	
200	
300	
400	
800	801, 802, 803, 804, 805, 806, 807, 808, 809, 812, 813, 814, 815, 816, 817, 818, 819, 821, 822, 825, 827, 830, 831, 834, 845, 836, 837, 859, 882, 883

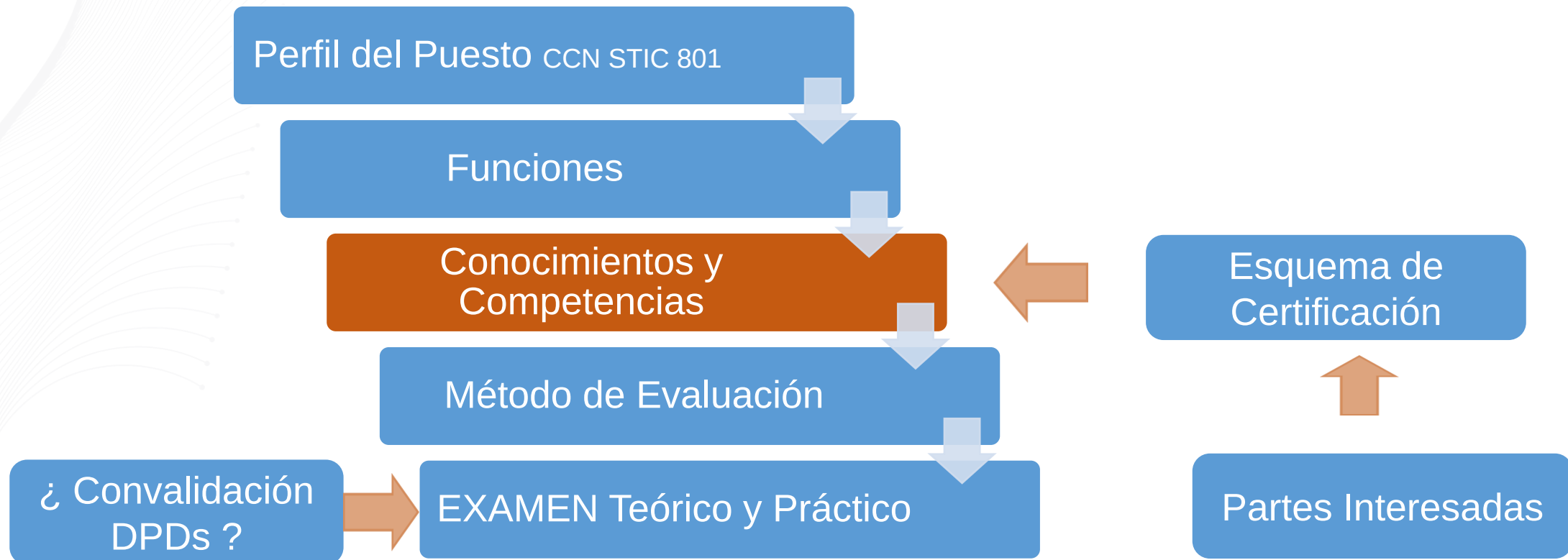
4. LA CERTIFICACION DE PERSONAS EN EL AMBITO DEL ENS

El Responsable de Seguridad: Competencias y Funciones



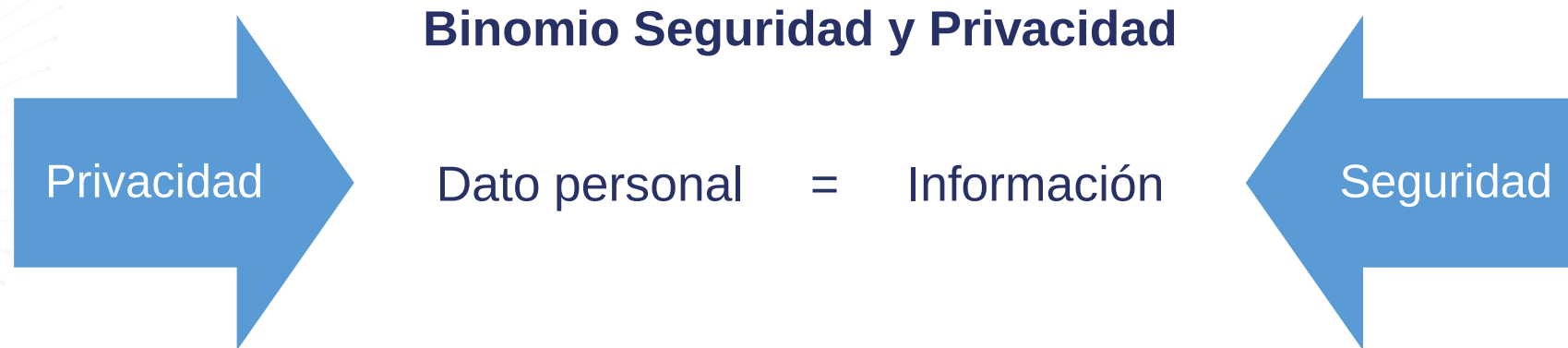
4. LA CERTIFICACION DE PERSONAS EN EL AMBITO DEL ENS

El Responsable de Seguridad: Esquema de Certificación



5. EL RESPONSABLE DE SEGURIDAD Y LA PRIVACIDAD

Responsable de Seguridad & Privacidad



Actualmente “todo” dato personal es un dato lógico

5. EL RESPONSABLE DE SEGURIDAD Y LA PRIVACIDAD

Responsable de Seguridad & Delegado de Protección de Datos

CCN-STIC-801

Esquema Nacional de Seguridad – Responsabilidades

6. La AEPD ha señalado la posibilidad de que el Delegado de Protección de Datos coincida con el Responsable de la Seguridad del ENS “en aquellas organizaciones que, por su tamaño y recursos, no pudieran observar dicha separación, sería admisible la designación como delegado de protección de datos de la persona que ejerciera las funciones de responsable de seguridad del ENS, siempre que en la misma concurren los requisitos de formación y capacitación previstos en el RGPD. Además, resultaría imprescindible adoptar todas las medidas organizativas, debidamente reflejadas en su Política de seguridad de la información, que garantice la necesaria independencia y la ausencia de conflicto de intereses, por lo que no podría recibir instrucciones respecto al desempeño de sus funciones como delegado de protección de datos, deberá responder directamente al más alto nivel jerárquico y no podrá participar en las decisiones relativas a los fines y medios del tratamiento. En todo caso, esta circunstancia, que como decíamos, tiene carácter excepcional, deberá evaluarse caso por caso, y deberá dejarse documentada dicha designación haciendo constar los motivos por lo que el organismo correspondiente no ha podido observar dicha separación de funciones así como las medidas que garantizan la necesaria independencia del delegado de protección de datos⁹.”

5. EL RESPONSABLE DE SEGURIDAD Y LA PRIVACIDAD

Responsable de Seguridad & Delegado de Protección de Datos

Tareas y Actividades

ENS	RGPD	Decisión	Ejecución	Supervisar	Asesorar
Elaborar políticas de seguridad. Desarrollar políticas de seguridad. Elaborar documento de aplicabilidad	Informar y asesorar (EVALUACIÓN DE IMPACTO)	X			X
Supervisar políticas de seguridad	Supervisar aplicación RGPD			X	
Capacitar	No existe esta función		X		
Notificación de incidentes	Cooperar con la autoridad de control, punto de contacto		X		

5. EL RESPONSABLE DE SEGURIDAD Y LA PRIVACIDAD

Responsable de Seguridad & Delegado de Protección de Datos

¿Qué le puede faltar a un responsable de seguridad para ser “Delegado de Protección de Datos” o Responsable de Protección de Datos?

Algunos conocimientos de carácter jurídico:

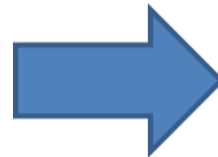
- Cláusulas informativas de derechos; muy estandarizadas (legalidad de las cesiones y comunicaciones de datos personales).
- Documentos contractuales con los encargados de los tratamientos; muy estandarizadas (incluso si al encargado del tratamiento se le exigen medidas de seguridad, se requieren conocimientos técnicos).
- Transferencias internacionales; incluso basta el consentimiento del interesado.
- Etc.

5. EL RESPONSABLE DE SEGURIDAD Y LA PRIVACIDAD

Responsable de Seguridad & Delegado de Protección de Datos

Desplazamiento de la función de Delegado de Protección de Datos
o del responsable de protección de datos

(20) Perfil jurídico

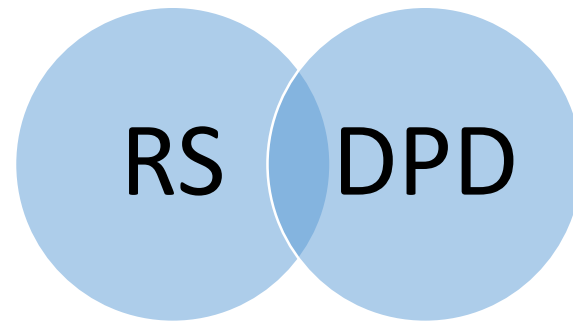


Perfil TIC (80)

5. EL RESPONSABLE DE SEGURIDAD Y LA PRIVACIDAD

Responsable de Seguridad & Delegado de Protección de Datos

Una propuesta de certificación de personas: RS + DPD



AEPD: ejercicio práctico sobre el ENS

CCN-ENS: ejercicio teórico/práctico sobre algunos aspectos “jurídicos”

6. CONCLUSIONES

La Certificación de Personas



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional