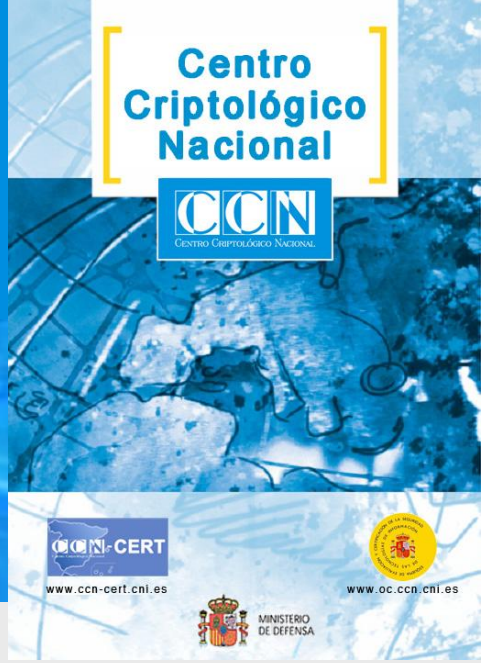


ESQUEMA NACIONAL DE SEGURIDAD

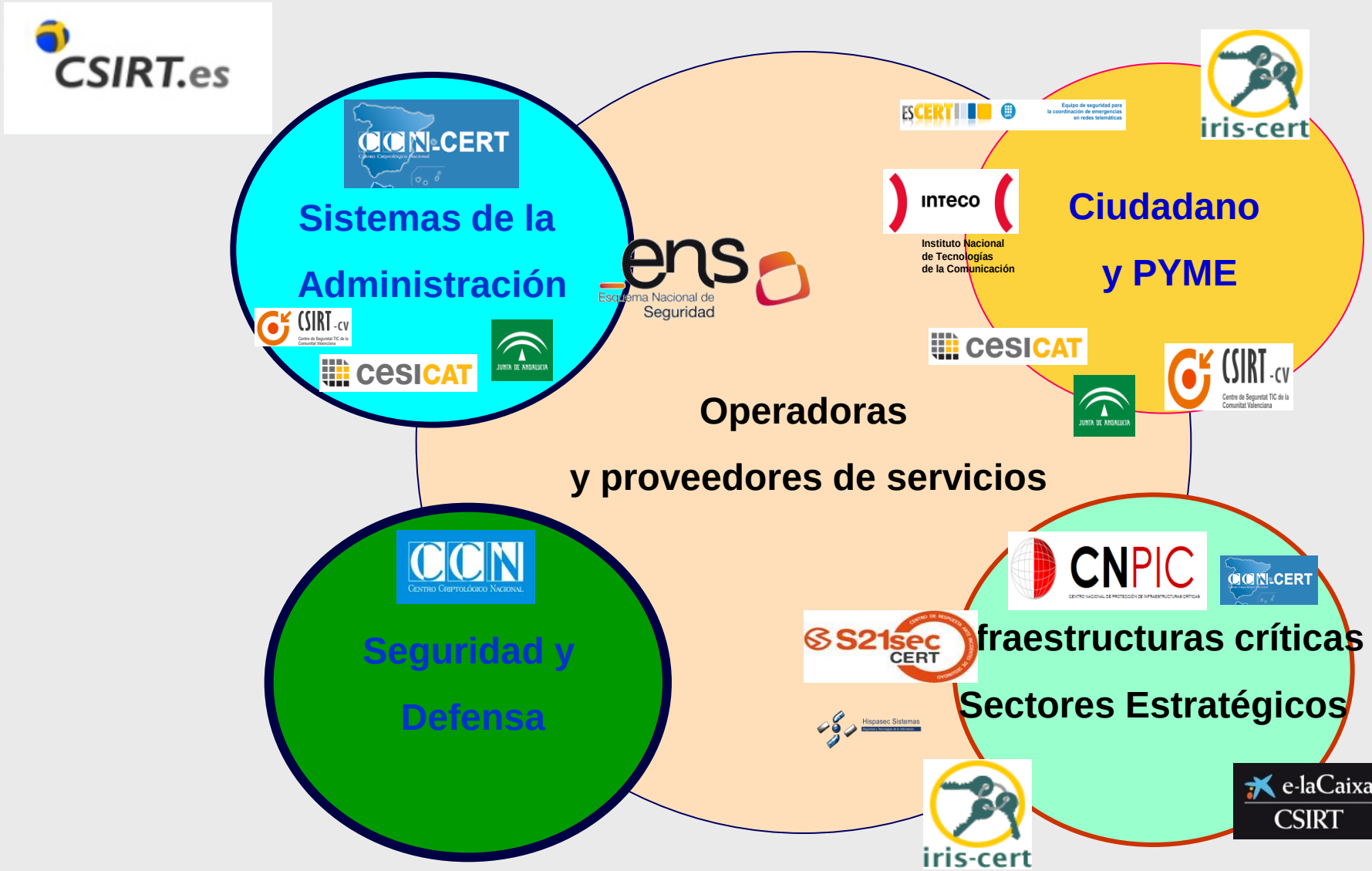
¿Cómo afecta el E.N.S. a los ISPs que prestan servicios a las Administraciones públicas?

Estrategia Española de Ciberseguridad

Madrid, mayo de 2012

SIN CLASIFICAR

Entornos de trabajo

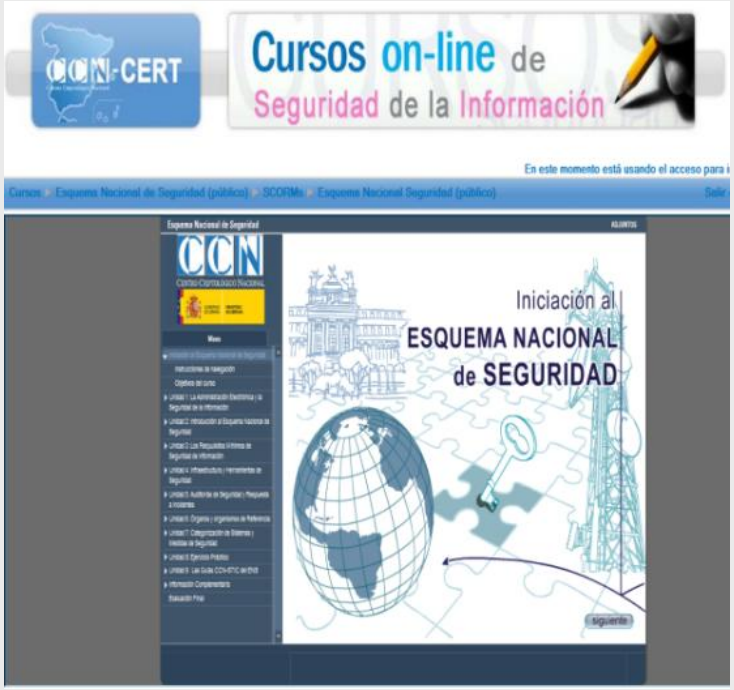


Índice

- Ámbito de aplicación del ENS
- Proveedores de servicios de Internet y el ENS
  - ENS – Servicios externos
  - Guías CCN-STIC
- Como afecta su aplicación.
- Estrategia Española Ciberseguridad
  - Estructura
  - Objetivos
  - Líneas de Acción
    - Cooperación público-privada

RD 3/2010

ESQUEMA NACIONAL DE SEGURIDAD



Abordar la adecuación

Artículo 27. Cumplimiento de requisitos mínimos.

1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las Administraciones públicas aplicarán las medidas de seguridad indicadas en el Anexo II, teniendo en cuenta:

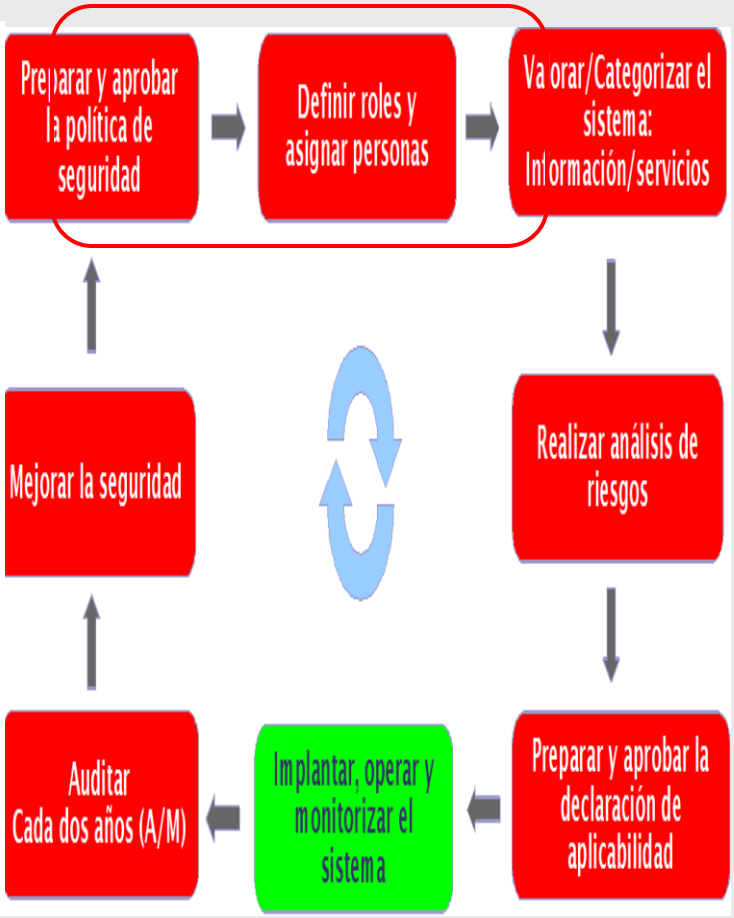
a) Los activos que constituyen el sistema.

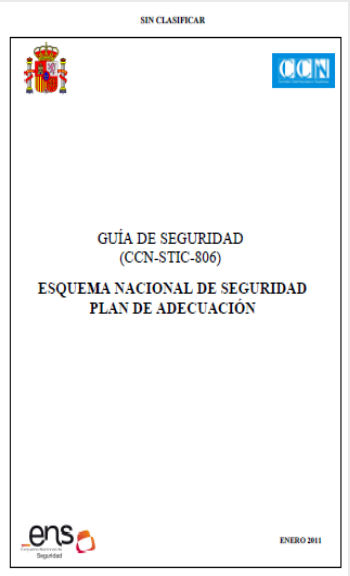
b) La categoría del sistema, según lo previsto en el artículo 43.

c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Cuando un sistema al que afecte el presente real decreto maneje datos de carácter personal le será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo, sin perjuicio de los requisitos establecidos en el Esquema Nacional de Seguridad.

3. Los medidas a las que se refieren los apartados 1 y 2 tendrán la condición de mínimos exigibles, y podrán ser ampliados por causa de la concurrencia indicada o del prudente arbitrio del responsable de la seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.




SIN CLASIFICAR

GUÍA DE SEGURIDAD
(CCN-STIC-806)

ESQUEMA NACIONAL DE SEGURIDAD
PLAN DE ADECUACIÓN

ENERO 2011

Esquema Nacional de Seguridad

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
				org	Marco organizativo
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización
				op	Marco operacional
				op.pl	Planificación
categoría	aplica	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	=	=	op.pl.2	Arquitectura de seguridad
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento / Gestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
I C A T	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local (local logon)
I C A T	aplica	+	=	op.acc.7	Acceso remoto (remote login)
				op.exp	Explotación
categoría	aplica	=	=	op.exp.1	Inventario de activos
categoría	aplica	=	=	op.exp.2	Configuración de seguridad
categoría	n.a.	aplica	=	op.exp.3	Gestión de la configuración

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
categoría	aplica	=	=	op.exp.4	Mantenimiento
categoría	n.a.	aplica	=	op.exp.5	Gestión de cambios
categoría	aplica	=	=	op.exp.6	Protección frente a código dañino
categoría	n.a.	aplica	=	op.exp.7	Gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.8	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	op.exp.9	Registro de la gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.10	Protección de los registros de actividad
categoría	aplica	+	=	op.exp.11	Protección de claves criptográficas
				op.ext	Servicios externos
categoría	n.a.	aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
categoría	n.a.	aplica	=	op.ext.2	Gestión diaria
D	n.a.	n.a.	aplica	op.ext.9	Medios alternativos
				op.cont	Continuidad del servicio
D	n.a.	aplica	=	op.cont.1	Análisis de impacto
D	n.a.	n.a.	aplica	op.cont.2	Plan de continuidad
D	n.a.	n.a.	aplica	op.cont.3	Pruebas periódicas
				op.mon	Monitorización del sistema
categoría	n.a.	n.a.	aplica	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas
				mp	Medidas de protección
				mp.if	Protección de las instalaciones e infraestructuras
categoría	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoría	aplica	=	=	mp.if.2	Identificación de las personas
categoría	aplica	=	=	mp.if.3	Acondicionamiento de los locales
D	aplica	+	=	mp.if.4	Energía eléctrica
D	aplica	=	=	mp.if.5	Protección frente a incendios
D	n.a.	aplica	=	mp.if.6	Protección frente a inundaciones
categoría	aplica	=	=	mp.if.7	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	mp.if.9	Instalaciones alternativas
				mp.per	Gestión del personal
categoría	n.a.	aplica	=	mp.per.1	Caracterización del puesto de trabajo
categoría	aplica	=	=	mp.per.2	Deberes y obligaciones

- **Marco organizativo:**
  - Política de seguridad.
  - Normativa de seguridad.
  - Procedimientos de seguridad.
  - Proceso de autorización.
- **Marco operacional:**
  - Planificación.
  - Control de acceso.
  - Explotación.
  - Servicios externos.
  - Continuidad del servicio.
  - Monitorización del sistema.
- **Marco de protección:**
  - Protección de las instalaciones e infraestructuras.
  - Gestión de personal.
  - Protección de los equipos.
  - Protección de las comunicaciones.
  - Protección de los soportes de información.
  - Protección de las aplicaciones informáticas.
  - Protección de la información.
  - Protección de los servicios.

ENS. SERVICIOS EXTERNOS (1)

- 4.4 Servicios externos [op.ext].
  - Cuando se utilicen recursos externos a la organización, sean servicios, equipos, instalaciones o personal, deberá tenerse en cuenta que la delegación se limita a las funciones.
  - La organización sigue siendo en todo momento **responsable de los riesgos** en que se incurre en la medida en que impacten sobre la información manejada y los servicios finales prestados por la organización.
  - La organización dispondrá las medidas necesarias para poder ejercer su responsabilidad y mantener el control en todo momento.
- 4.4.1 Contratación y acuerdos de nivel de servicio [op.ext.1].
  - Previa a la utilización de recursos externos se establecerán contractualmente las características del servicio prestado y las responsabilidades de las partes. Se detallará **lo que se considera calidad mínima del servicio prestado y las consecuencias de** su incumplimiento.

todas		
básica	media	alta
no aplica	aplica	=

ENS. SERVICIOS EXTERNOS (2)

- 4.4.2 Gestión diaria [op.ext.2].
  - a) Un **sistema** rutinario para **medir el cumplimiento de las obligaciones de servicio y el procedimiento para neutralizar cualquier desviación** fuera del margen de tolerancia acordado ([op.ext.1]).
  - b) El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo.
  - c) El mecanismo y los procedimientos de **coordinación** en caso de **incidencias y desastres** (ver [op.exp.7]).

todas		
básica	media	alta
no aplica	aplica	=

- 4.4.3 Medios alternativos [op.ext.9].
  - Estará prevista la provisión del servicio por medios alternativos en caso de indisponibilidad del servicio contratado. El servicio alternativo disfrutará de las mismas garantías de seguridad que el servicio habitual

D		
bajo	medio	alto
no aplica	no aplica	aplica

todas		
básica	media	alta
no aplica	aplica	=

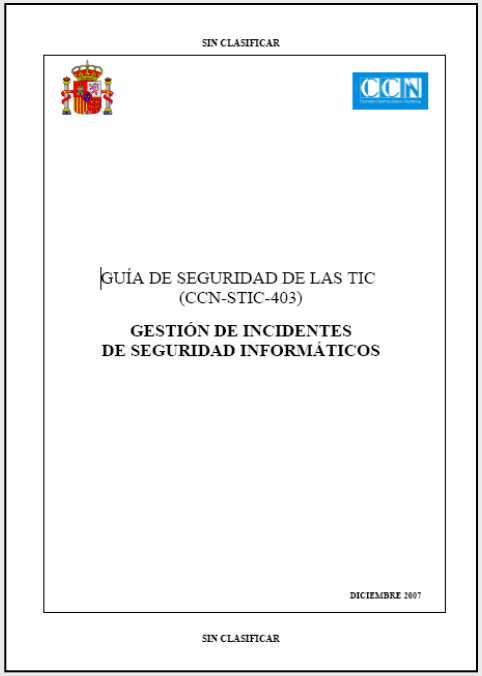
- 4.5 Continuidad del servicio [op.cont].
  - 4.5.1 Análisis de impacto [op.cont.1].
    - a) Los requisitos de disponibilidad de cada servicio medidos como el impacto de una interrupción durante un cierto periodo de tiempo.
    - b) Los elementos que son críticos para la prestación de cada servicio.
  - 4.5.2 Plan de continuidad [op.cont.2].
    - Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Este plan contemplará los siguientes aspectos
    - …//….

D		
bajo	medio	alto
no aplica	no aplica	aplica

  - 4.5.3 Pruebas periódicas [op.cont.3].
    - Se realizarán pruebas periódicas para localizar y, corregir en su caso, los errores o deficiencias que puedan existir en el plan de continuidad

Normativa

- 189 documentos, normas, instrucciones, guías y recomendaciones
  - (25 pendientes de su aprobación)
- Nueva serie 800: ESQUEMA NACIONAL DE SEGURIDAD
  - **18 Guías**
- Nueva clasificación:
  - Cumplen con el ENS
  - Adaptables al ENS


SIN CLASIFICAR

GUÍA DE SEGURIDAD DE LAS TIC
(CCN-STIC-403)

GESTIÓN DE INCIDENTES
DE SEGURIDAD INFORMÁTICOS

DICIEMBRE 2007

SIN CLASIFICAR

Guías previstas en ENS – SERIE 800

- 801 Responsabilidades y Funciones en el ENS feb-11
- 802 Auditoría del Esquema Nacional de Seguridad jun-10
- 803 Valoración de Sistemas en el ENS ene-11
- 804 Medidas de Implantación del ENS (BORRADOR) jul-10
- 805 Política de Seguridad de la Información sep-11
- 806 Plan de Adecuación del ENS ene-11
- **807 Criptología de Empleo en el ENS sep-11**
- **808 Verificación del Cumplimiento de las Medidas en el ENS (BORRADOR) oct-10**
- 809 Declaración de conformidad del ENS (BORRADOR) jul-10
- 810 Guía de Creación de CERT,s (BORRADOR) sep-11
- **811 Interconexión en el ENS (BORRADOR) sep-11**
- 812 Seguridad en Servicios Web en el ENS (BORRADOR) oct-11
- 813 Componentes Certificados en el ENS
- 814 Seguridad en Servicio de Correo en el ENS (BORRADOR) ago-11
- **815 Indicadores y Métricas en el ENS (BORRADOR) dic-11**
- 816 Seguridad en Redes Inalámbricas en el ENS
- **817 Gestión de Incidentes de Seguridad en el ENS …. Feb -12 + ANEXO 403**
- 818 Herramientas de seguridad en el ENS

- **819 Seguridad en VPN**
- **820 Req Cloud computing**
- **821 Seguridad en DNS**
- **822 Ejemplos POS**
- **823 Externalización**

RD 3/2010
ESQUEMA NACIONAL DE SEGURIDAD

- **COMO AFECTA A LOS ISP,S.**
- **ASPECTOS LEGALES**

Ambito de aplicación del ENS

- **Art. 3 del RD 3/2010 de 8 de enero.**
  - El ámbito de aplicación del presente real decreto será el establecido en el **artículo 2 de la Ley 11/2007**, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
  - Están excluidos los sistemas que tratan información clasificada.
- **Art. 2 de la Ley 11/2007, de 22 de junio.**
  - La Ley es de aplicación:
    - A las Administraciones públicas (AGE, CC.AA, EAL)
    - Entidades de derecho públicos vinculadas o dependientes de las AA.PP.
    - A los ciudadanos en sus relaciones con las AA.PP.
    - A las relaciones entre las distintas Administraciones.
- **Casos en los no que resulta de aplicación el E.N.S.**
  - a) Art. 2.2. de la Ley 11/2007, de 22 de junio. La Ley no será de aplicación a las actividades que se desarrollen en régimen de derecho privado.
  - b) Art. 30 del Real Decreto 2/2010 (ENS)- Las AAPP podrán determinar aquellos sistemas que no le sea de aplicación por:
    - Tratarse de sistemas no relacionados con el ejercicio de derechos ni con el cumplimiento de deberes por medios electrónicos.
    - Ni con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo

PRESTADOR DE SERVICIOS DE INTERNET

- **Servicios de Sociedad de la Información.**
  - Todo servicio prestado normalmente a título, a distancia, por vía electrónica y a petición individual de un destinatario de servicios. El concepto comprende también los servicios no remunerados por sus destinatarios, en la medidas en que constituyan una actividad económica para el prestador del servicio (Ley de Sociedad de la Información).
- **Los ISPs un caso particular.**
  - Dentro de la amplitud los prestadores de servicios de la sociedad de la información están los **prestadores de servicios de Internet (ISPs)** para referirse a una categoría más reducida de prestadores que son los que proporcionan los servicios necesarios para hacer posible el uso de Internet, entre los que destacan los **proveedores de acceso** y los **prestadores de servicios de alojamiento**.
- **Art. 11, 13 a 17 y Anexo de la Ley 34/2002, de 11 de julio LSSI.**
  - Son objeto de **regulación específica por cuanto se refiere a su responsabilidad**, los intermediarios que proveen servicios de Internet, los que prestan servicios de transmisión de datos por redes de telecomunicaciones, aquellos que realizan la copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrador por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet

RÉGIMEN DE LA PRESTACIÓN DE SERVICIOS DE LOS ISPs A LAS AAPP

- **Régimen de los contratos administrativos y régimen de los contratos privados.**
  - El régimen jurídico de los contratos celebrados con la Administración no es unitario o es unitario y puro, sino que es variable y mixto, apareciendo siempre mezclado el **Derecho Administrativo y el Derecho Privado.**
- **Mezcla de Derecho Administrativo y Derecho Privado en los contratos con las AA.PP. Reglas específicas de cada contrato son las que definen el régimen concreto de cada contrato.**
  - Partiendo de ese régimen mixto de los contratos con la Administración, **lo realmente determinante son las reglas específicas de cada contrato**, porque son esas reglas y no su calificación como administrativo o como privado, **las que definen su concreto régimen jurídico**.
- **Contratos más comunes de los ISPs:**
  - Acceso a Internet.
  - Desarrollo de páginas web.
  - Adquisición de contenidos.
  - Alojamiento de sitio web
  - Creación de sitio compartido
  - Contratos publicitarios

LA CONTRATACIÓN DE RECURSOS EXTERNOS EN EL E.N.S.

- Punto 4.4. del Anexo II del Real Decreto 3/2010, de 8 de enero E.N.S.
  - Exigencia de establecer contractualmente el servicio prestado.
  - Cesión de funciones.
- Responsabilidad :
  - De la Administración contratante.
    - **La organización sigue siendo en todo momento responsable de los riesgos en que se incurre en la medida en que impacten sobre la información manejada y los servicios finales prestados** por la organización.
  - Del ISP frente a la Administración.
    - **Los ISPs serán responsable frente a la Administración contratante de los incumplimientos contractuales.**
- Medidas de control de la Administración contratante.

CONTRATOS DE ADHESIÓN, CONDICIONES GENERALES DE CONTRATACIÓN Y CÓDIGO DE CONDUCTA Y BUENAS PRÁCTICAS.

- **Contratos de adhesión.**
  - Aquellos contratos que las condiciones son obra de una sola parte quedando en vínculo contractual de la otra parte formalizado mediante un simple acto de aceptación.
- **Contratos celebrados en base a condiciones generales de contratación**
  - Son contratos celebrados en base a unas condiciones generales elaboradas por una empresa o grupo y propuesta como patrón para los clientes que contraten con ellos.
  - En España están regulados por la Ley 7/1998, de 13 de abril sobre condiciones generales de contratación que, en su artículo 4 dice, que **no se aplicará a los contratos administrativos**
- **Códigos de Conducta y Buenas Prácticas.**
  - **art. 6 y 16 de la Directiva 2005/29/CE.**
    - **Acuerdo conjunto de normas** no impuestas por disposiciones legales, en las que se define el **comportamiento de aquellos comerciantes que se comprometen a cumplir un código en relación con una práctica comercial o sectores económicos concretos**. En la ordenación de Internet y las actividades de comercio electrónico son relevantes.
  - **art. 18 de la LSSI**
    - Las Administraciones públicas impulsarán a través de la coordinación y el asesoramiento, la elaboración y aplicación de **códigos de conducta voluntarios.**
  - **art. 5 Ley de Competencia Desleal**
    - Considera **desleal el incumplimiento de compromisos previstos en un código de conducta.**
  - **art. 37 del RD 1163/2005, distintivo público de confianza en línea.**
    - Carácter voluntario. Su finalidad es elevar el **nivel de protección de los consumidores**

CONCLUSIONES

- El ENS afecta de modo indirecto a los prestadores de servicios de Internet.

- La Administración contratante establece las obligaciones de los ISPs mediante contrato.
  - En el clausulado del contrato se establecen los requerimientos contractuales.
- Las Administraciones públicas están obligadas a establecer los **requerimientos atendiendo a lo dispuesto en el ENS**, cuando sea de aplicación.
- Las obligaciones de los ISPs para con el ENS no provienen directamente de su Real Decreto regulador, **sino del contrato celebrado con la Administración**.
- Los ISPs responderán de sus incumplimientos ante la Administración contratante.

CONCLUSIONES GENERALES

- **La Estrategia Española de Ciberseguridad reforzará la aplicación del ENS.**

- **Necesidad de una cooperación PUBLICO-PRIVADA más estrecha.**
  - **Defensa común.**
  - **Intercambio de información.**
  - **Desde diferentes aproximaciones**
  - **Código de Buenas Prácticas para los ISP,s**

- **Interceptación legal de comunicaciones.**
  - **Mejorar la eficiencia de los organismo competentes.**

- **Los ISPs son actores fundamentales en la SEGURIDAD EN EL CIBERESPACIO en ESPAÑA.**

Gracias

- **CÓMO CONTACTAR:**
  - ccn@cni.es
  - **INCIDENTES**
    - incidentes@ccn-cert.cni.es
  - **SISTEMAS ALERTA TEMPRANA**
    - sondas@ccn-cert.cni.es
    - redsara@ccn-cert.cni.es
    - carmen@ccn-cert.cni.es
  - **GENERAL**
    - info@ccn-cert.cni.es
    - ens@ccn-cert.cni.es

APENDICE NORMATIVO

a. Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

b. Ley 30/2002, de 30 de octubre, de Contratos del Sector Público.

c. Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter Personal.

d. Ley 34/2002, de 11 de julio, de servicios de la Sociedad de la Información y de comercio electrónico.

e. Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios Públicos.

f. 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.

g. Ley 3/1991, de 10 de enero de competencia desleal, modificada por Ley 29/2009, de 30 de diciembre.

h. Real Decreto 1163/2005, de 30 de septiembre, que regula el distintivo público de confianza en los servicios de la sociedad de la información