



## ÍNDICE

<b>1</b>	<b>INTRODUCCIÓN</b>	<b>3</b>
<b>2</b>	<b>FINALIDAD</b>	<b>3</b>
<b>3</b>	<b>METODOLOGÍA</b>	<b>3</b>
<b>3.1</b>	<b>NIVELES DE MADUREZ</b>	<b>3</b>
<b>3.2</b>	<b>PERFILES DE SEGURIDAD EVALUADOS</b>	<b>4</b>
<b>3.3</b>	<b>ÍNDICE DE CUMPLIMIENTO (IC)</b>	<b>5</b>
<b>3.4</b>	<b>ÍNDICE DE MEJORA (IME)</b>	<b>5</b>
<b>3.5</b>	<b>ÍNDICE DE MADUREZ (IM)</b>	<b>6</b>
<b>4</b>	<b>PARTICIPACIÓN</b>	<b>7</b>
<b>5</b>	<b>RESUMEN EJECUTIVO</b>	<b>7</b>
<b>5.1</b>	<b>DEFICIENCIAS DEL SISTEMA</b>	<b>7</b>
<b>5.2</b>	<b>OPORTUNIDADES DE MEJORA</b>	<b>7</b>
<b>6</b>	<b>CONCLUSIONES</b>	<b>7</b>
<b>7</b>	<b>ANEXO A. MEDIDAS DEL ANEXO II DEL ENS</b>	<b>8</b>
<b>8</b>	<b>ANEXO B. ANÁLISIS Y GESTIÓN DE RIESGOS</b>	<b>14</b>
<b>9</b>	<b>ANEXO C. ACTIVIDADES ORGANIZATIVAS</b>	<b>15</b>
<b>10</b>	<b>ANEXO D. RECURSOS</b>	<b>16</b>
<b>11</b>	<b>ANEXO E. INTERCONEXIÓN CON OTROS SISTEMAS</b>	<b>17</b>
<b>12</b>	<b>ANEXO F. APLICACIÓN DE LA SEGURIDAD</b>	<b>18</b>
<b>13</b>	<b>ANEXO G. GESTIÓN DE INCIDENTES</b>	<b>21</b>
<b>14</b>	<b>ANEXO H. AUDITORÍAS</b>	<b>22</b>
<b>15</b>	<b>INDICADORES CLAVE DE RIESGO (KRI)</b>	<b>23</b>

# 1 INTRODUCCIÓN

El Informe Nacional del Estado de la Seguridad (INES) de los sistemas de las tecnologías de la información y la comunicación responde al requerimiento de elaborar un perfil general del estado de la seguridad de las Administraciones públicas, recogido en el artículo 35 del Real Decreto 3/2010, de 8 de enero, modificado por el RD 951/2015, de 23 de octubre, por el que se regula el Esquema Nacional de Seguridad (ENS), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

El Centro Criptológico Nacional articulará los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación.

# 2 FINALIDAD

Mediante el presente informe, el organismo puede conocer el estado de la seguridad de sus sistemas, identificar deficiencias en la ciberseguridad, cotejar su posición particular respecto de la media nacional y la media del su propio ámbito (Administración General del Estado, Comunidades Autónomas, Entidades Locales y Universidades) y tomar decisiones estratégicas que le permitan llevar a cabo la gobernanza de la ciberseguridad.

# 3 METODOLOGÍA

Para la recogida de datos de este informe se ha empleado la herramienta INES (Informe Nacional del Estado de Seguridad) destinada a la gobernanza de la ciberseguridad nacional, según los criterios establecidos en la actualizada guía CCN-STIC-824 Informe del Estado de Seguridad.

Las métricas e indicadores presentados en esta guía derivan del marco descrito en la guía CCN-STIC-815 ENS Métricas e Indicadores.

## 3.1 NIVELES DE MADUREZ

Los controles de las diferentes medidas de seguridad se evalúan mediante un nivel de madurez y dependiendo de la categoría del sistema de que se trate se establece cual debe ser el nivel mínimo requerido, según se detalla a continuación:

NIVEL DE MADUREZ		DESCRIPCIÓN DEL NIVEL
Nivel	%	
L0	0	<b>Inexistente.</b> Esta salvaguarda no existe en este momento.
L1	10	<b>Inicial/ad hoc.</b> Se hace cuando se considera adecuado, pero no está establecido.
L2	50	<b>Reproducible, pero intuitivo.</b> Se realiza, pero no está formalizado documentalmente.
L3	80	<b>Proceso definido.</b> Se realiza y está definido documentalmente (procedimientos).

NIVEL DE MADUREZ		DESCRIPCIÓN DEL NIVEL
Nivel	%	
L4	90	<b>Gestionado y medible.</b> Se están gestionando y son susceptibles de ser medidas.
L5	100	<b>Optimizado.</b> La medida está definida, medida y se aplica proceso de mejora y optimización.

Figura 1.- Niveles de madurez y equivalencia en %

CATEGORÍA DEL SISTEMA	NIVEL MÍNIMO DE MADUREZ REQUERIDO
BÁSICA	L2 - Reproducible, pero intuitivo (50%)
MEDIA	L3 - Proceso definido (80%)
ALTA	L4 - Gestionado y medible (90%)

Figura 2.- Niveles mínimos de madurez del sistema requeridos en el Esquema Nacional de Seguridad

### 3.2 PERFILES DE SEGURIDAD EVALUADOS

Sobre los perfiles de seguridad utilizados en este estudio se han realizado las siguientes consideraciones:

- **Perfil ENS (ANEXO II del RD 3/2010).** El tanto por ciento (%) de cumplimiento de este perfil indicará el nivel de cumplimiento del ENS por parte del organismo. Se han valorado todos los aspectos del marco ORGANIZATIVO, marco OPERACIONAL y medidas de PROTECCIÓN.
  - **Marco ORGANIZATIVO.** Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad. Se valora la existencia de una política de seguridad, de una organización de seguridad de soporte, de normativa y procedimientos.
  - **Marco OPERACIONAL.** Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes. Se valoran los aspectos de planificación, control de accesos, operación, servicios externos, continuidad del servicio y monitorización del sistema.
  - **Medidas de PROTECCIÓN.** Se centra en las medidas para proteger activos concretos del sistema como instalaciones e infraestructuras, personal, equipos, comunicaciones, soportes de información, aplicaciones informáticas, información y servicios.



Figura 3.- Medidas de seguridad del ENS

- **Gestión de Incidentes (CCN-STIC-817).** La información asociada a la gestión de incidentes es registrada en LUCIA a través de los datos aportados por los servicios de alerta temprana del CCN-CERT (SAT SARA y SAT INET) y por el responsable de seguridad, en caso de contar con una instancia local en el organismo. Dicha información puede ser importada en INES.

### 3.3 ÍNDICE DE CUMPLIMIENTO (IC)

El índice de cumplimiento es el valor agrupado de todas las medidas de seguridad que son de aplicación, ponderadas teniendo en cuenta la categoría del sistema.

El índice de cumplimiento de Diputación de Castellón es:

	Índice de Cumplimiento
<b>BÁSICA</b>	95.00
<b>MEDIA</b>	91.53
<b>ALTA</b>	0.00

Figura 4.- Índice de cumplimiento de Diputación de Castellón

	Índice de Cumplimiento
<b>BÁSICA</b>	84
<b>MEDIA</b>	68.55
<b>ALTA</b>	64.05

Figura 5.- Mediana global del índice de cumplimiento

	Índice de Cumplimiento
BÁSICA	87.11
MEDIA	62.66
ALTA	49.15

Figura 6.- Mediana global del índice de cumplimiento para su ámbito

El valor objetivo a conseguir es de 100%.

### 3.4 ÍNDICE DE MEJORA (IME)

El Índice de Mejora representa el esfuerzo en seguridad necesario para alcanzar un Índice de Cumplimiento adecuado. El valor es 100-IC en %.

	Índice de Mejora
BÁSICA	5
MEDIA	8.47
ALTA	100

Figura 7.- Índice de mejora de Diputación de Castellón

	Índice de Mejora
BÁSICA	16
MEDIA	31.45
ALTA	35.95

Figura 8.- Mediana global del índice de mejora

	Índice de Mejora
BÁSICA	12.89
MEDIA	37.34
ALTA	50.85

Figura 9.- Mediana global del índice de mejora para su ámbito

Porcentajes de mejora, hasta alcanzar un índice de cumplimiento óptimo, por categorías.



Figura 10.- Resultados de Mejora Continua para categoría BÁSICA



Figura 11.- Resultados de Mejora Continua para categoría MEDIA



Figura 12.- Resultados de Mejora Continua para categoría ALTA

### 3.5 ÍNDICE DE MADUREZ (IM)

El índice de madurez es el valor agrupado de todas las medidas de seguridad que son de aplicación al sistema, sin ponderar.

	Índice de Madurez
BÁSICA	81.20
MEDIA	80.67
ALTA	0.00



Figura 13.- Índice de madurez de Diputación de Castellón

	Índice de Madurez
<b>BÁSICA</b>	46.86
<b>MEDIA</b>	56.02
<b>ALTA</b>	59.07

Figura 14.- Mediana global del índice de madurez

	Índice de Madurez
<b>BÁSICA</b>	49.33
<b>MEDIA</b>	50.05
<b>ALTA</b>	44.24

Figura 15.- Mediana global del índice de madurez para su ámbito

Sin embargo, lo recomendado es conseguir 100%.

## 4 PARTICIPACIÓN

El número de organismos que han registrado datos en INES dentro de su agrupación (Diputación o cabildo) es de 58.

El número de sistemas es el siguiente:

- 0 de categoría ALTA.
- 1 de categoría MEDIA.
- 1 de categoría BÁSICA.

A continuación, se presentan los niveles asociados a las dimensiones de seguridad:

Dimensión	Valor Registrado		
	BÁSICA	MEDIA	ALTA
Nivel de la Confidencialidad	No aplica	Medio	n.a
Nivel de la Integridad	No aplica	Bajo	n.a
Nivel de la Trazabilidad	No aplica	Medio	n.a
Nivel de la Autenticidad	No aplica	Bajo	n.a

Dimensión	Valor Registrado		
	BÁSICA	MEDIA	ALTA
Nivel de la Disponibilidad	Bajo	Medio	n.a

## 5 RESUMEN EJECUTIVO

### 5.1 DEFICIENCIAS DEL SISTEMA

### 5.2 OPORTUNIDADES DE MEJORA

## 6 CONCLUSIONES

## 7 ANEXO A. MEDIDAS DEL ANEXO II DEL ENS

Se presentan los niveles de cumplimiento para cada una de las 75 medidas del Esquema Nacional de Seguridad:

### [ORG] MARCO ORGANIZATIVO

Marco organizativo		Madurez o n.a. <sup>1</sup>		
[Org]	Medidas	BÁSICA	MEDIA	ALTA
[org.1]	Política de seguridad	100	100	n.a
[org.2]	Normativa de seguridad	80	80	n.a
[org.3]	Procedimientos de seguridad	80	80	n.a
[org.4]	Proceso de autorización	80	80	n.a

### [OP] MARCO OPERACIONAL

Marco operacional		Madurez o n.a.		
[Op]	Medidas	BÁSICA	MEDIA	ALTA
<b>[op.pl]</b>	<b>Planificación</b>	<b>58.00</b>	<b>58.00</b>	<b>n.a</b>
[op.pl.1]	Análisis de riesgos	90	90	n.a
[op.pl.2]	Arquitectura de seguridad	50	50	n.a
[op.pl.3]	Adquisición de nuevos componentes	50	50	n.a
[op.pl.4]	Dimensionamiento / Gestión de capacidades	50	50	n.a
[op.pl.5]	Componentes certificados	50	50	n.a
<b>[op.acc]</b>	<b>Control de acceso</b>	<b>82.86</b>	<b>82.86</b>	<b>n.a</b>
[op.acc.1]	Identificación	90	90	n.a
[op.acc.2]	Requisitos de acceso	50	50	n.a
[op.acc.3]	Segregación de funciones y tareas	90	90	n.a

12 n.a. Acrónimo que se lee como “no aplica” o “no es aplicable”. Se emplea cuando una cierta medida de seguridad no es relevante en el sistema. Por ejemplo, no hay nada que decir del correo electrónico si el sistema no emplea este servicio.

Marco operacional		Madurez o n.a.		
[Op]	Medidas	BÁSICA	MEDIA	ALTA
[op.acc.4]	Proceso de gestión de derechos de acceso	90	90	n.a
[op.acc.5]	Mecanismo de autenticación	90	90	n.a
[op.acc.6]	Acceso local	80	80	n.a
[op.acc.7]	Acceso remoto	90	90	n.a
<b>[op.exp]</b>	<b>Explotación</b>	<b>86.36</b>	<b>86.36</b>	<b>n.a</b>
[op.exp.1]	Inventario de activos	90	90	n.a
[op.exp.2]	Configuración de seguridad	90	90	n.a
[op.exp.3]	Gestión de la configuración	80	80	n.a
[op.exp.4]	Mantenimiento	80	80	n.a
[op.exp.5]	Gestión de cambios	80	80	n.a
[op.exp.6]	Protección frente a código dañino	90	90	n.a
[op.exp.7]	Gestión de incidentes	80	80	n.a
[op.exp.8]	Registro de la actividad de los usuarios	90	90	n.a
[op.exp.9]	Registro de la gestión de incidentes	90	90	n.a
[op.exp.10]	Protección de los registros de actividad	90	90	n.a
[op.exp.11]	Protección de claves criptográficas	90	90	n.a
<b>[op.ext]</b>	<b>Servicios externos</b>	<b>83.33</b>	<b>83.33</b>	<b>n.a</b>
[op.ext.1]	Contratación y acuerdos de nivel de servicio	80	80	n.a
[op.ext.2]	Gestión diaria	80	80	n.a
[op.ext.9]	Medios alternativos	90	90	n.a
<b>[op.cont]</b>	<b>Continuidad del servicio</b>	<b>80.00</b>	<b>80.00</b>	<b>n.a</b>
[op.cont.1]	Análisis de impacto	80	80	n.a
[op.cont.2]	Plan de continuidad	80	80	n.a
[op.cont.3]	Pruebas periódicas	80	80	n.a

Marco operacional		Madurez o n.a.		
[Op]	Medidas	BÁSICA	MEDIA	ALTA
<b>[op.mon]</b>	<b>Monitorización del sistema</b>	<b>90.00</b>	<b>90.00</b>	<b>n.a</b>
[op.mon.1]	Detección de intrusión	90	90	n.a
[op.mon.2]	Sistema de métricas	90	90	n.a

### [MP] MEDIDAS DE PROTECCIÓN

Medidas de protección		Madurez o n.a.		
[mp]	Medidas	BÁSICA	MEDIA	ALTA
<b>[mp.if]</b>	<b>Protección de las instalaciones e infraestructuras</b>	<b>92.50</b>	<b>92.50</b>	<b>n.a</b>
[mp.if.1]	Áreas separadas y con control de acceso	100	100	n.a
[mp.if.2]	Identificación de las personas	90	90	n.a
[mp.if.3]	Acondicionamiento de los locales	90	90	n.a
[mp.if.4]	Energía eléctrica	90	90	n.a
[mp.if.5]	Protección frente a incendios	90	90	n.a
[mp.if.6]	Protección frente a inundaciones	90	90	n.a
[mp.if.7]	Registro de entrada y salida de equipamiento	100	100	n.a
[mp.if.9]	Instalaciones alternativas	90	90	n.a
<b>[mp.per]</b>	<b>Gestión del personal</b>	<b>42.00</b>	<b>42.00</b>	<b>n.a</b>
[mp.per.1]	Caracterización del puesto de trabajo	10	10	n.a
[mp.per.2]	Deberes y obligaciones	90	90	n.a
[mp.per.3]	Concienciación	10	10	n.a
[mp.per.4]	Formación	10	10	n.a
[mp.per.9]	Personal alternativo	90	90	n.a

Medidas de protección		Madurez o n.a.		
[mp]	Medidas	BÁSICA	MEDIA	ALTA
<b>[mp.eq]</b>	<b>Protección de los equipos</b>	<b>85.00</b>	<b>85.00</b>	<b>n.a</b>
[mp.eq.1]	Puesto de trabajo despejado	80	80	n.a
[mp.eq.2]	Bloqueo de puesto de trabajo	90	90	n.a
[mp.eq.3]	Protección de equipos portátiles	80	80	n.a
[mp.eq.9]	Medios alternativos	90	90	n.a
<b>[mp.com]</b>	<b>Protección de las comunicaciones</b>	<b>92.00</b>	<b>92.00</b>	<b>n.a</b>
[mp.com.1]	Perímetro seguro	100	100	n.a
[mp.com.2]	Protección de la confidencialidad	90	90	n.a
[mp.com.3]	Protección de la autenticidad y de la integridad	90	90	n.a
[mp.com.4]	Segregación de redes	90	90	n.a
[mp.com.9]	Medios alternativos	90	90	n.a
<b>[mp.si]</b>	<b>Protección de los soportes de información</b>	<b>70.00</b>	<b>62.00</b>	<b>n.a</b>
[mp.si.1]	Etiquetado	80	80	n.a
[mp.si.2]	Criptografía	10	10	n.a
[mp.si.3]	Custodia	80	80	n.a
[mp.si.4]	Transporte	100	60	n.a
[mp.si.5]	Borrado y destrucción	80	80	n.a
<b>[mp.sw]</b>	<b>Protección de las aplicaciones informáticas</b>	<b>85.00</b>	<b>85.00</b>	<b>n.a</b>
[mp.sw.1]	Desarrollo	90	90	n.a
[mp.sw.2]	Aceptación y puesta en servicio	80	80	n.a
<b>[mp.info]</b>	<b>Protección de la información</b>	<b>91.43</b>	<b>91.43</b>	<b>n.a</b>
[mp.info.1]	Datos de carácter personal	90	90	n.a
[mp.info.2]	Calificación de la información	90	90	n.a
[mp.info.3]	Cifrado	90	90	n.a
[mp.info.4]	Firma electrónica	90	90	n.a

Medidas de protección		Madurez o n.a.		
[mp]	Medidas	BÁSICA	MEDIA	ALTA
[mp.info.5]	Sellos de tiempo	90	90	n.a
[mp.info.6]	Limpieza de documentos	90	90	n.a
[mp.info.9]	Copias de seguridad ( <i>backup</i> )	100	100	n.a
<b>[mp.s]</b>	<b>Protección de los servicios</b>	<b>87.50</b>	<b>87.50</b>	<b>0</b>
[mp.s.1]	Protección del correo electrónico	90	90	n.a
[mp.s.2]	Protección de servicios y aplicaciones web	80	80	n.a
[mp.s.8]	Protección frente a la denegación de servicio	90	90	n.a
[mp.s.9]	Medios alternativos	90	90	n.a

### PROCESOS CRÍTICOS

Dentro del ámbito del ENS, se definen una serie de procesos críticos, entendidos como medidas independiente o agrupaciones de medidas por tipología. Los valores asociados a dichos procesos críticos, en función de las medidas del Anexo II del ENS, son las siguientes:

Proceso crítico	Madurez		
	Bajo	Medio	Alto
<b>Proceso de autorización</b> [org.4]	80	80	n.a
<b>Análisis de riesgos</b> [op.pl.1]	90	90	n.a
<b>Gestión de derechos de acceso</b> [op.acc.4]	90	90	n.a
<b>Gestión de incidentes</b> [op.exp.7]	80	80	n.a
<b>Concienciación y Formación</b> [mp.per.3 + mp.per.4]	10	10	n.a
<b>Configuración de seguridad y gestión de cambios</b> [op.exp.4 + op.exp.5]	80	80	n.a
<b>Continuidad de operaciones</b> [op.cont.1 + op.cont.2 + op.cont.3 + mp.if.9 + mp.per.9 + mp.eq.9 + mp.com.9 + mp.info.9 + mp.s.9 + op.ext.9]	88	88	n.a

Para aquellos procesos constituidos por más de una medida, el valor asociado a dicho proceso se calcula como la media de las medidas que los constituyen.

## 8 ANEXO B. ANÁLISIS Y GESTIÓN DE RIESGOS

La información que se ha registrado en relación a la realización de análisis de riesgos es la siguiente:

Análisis y Gestión de Riesgos	Valor Registrado
Dispone de Análisis de riesgos	Si
El análisis de riesgos abarca todos los sistemas declarados	Si
Dispone de AR en lenguaje natural, realizado como exposición textual	Si
Dispone de AR semiformal, usando lenguaje específico y presentación con tablas	Si
Dispone de AR formal, usando lenguaje específico y con metodología reconocida internacionalmente	Si
Número de activos totales en el análisis de riesgos	185
Número de activos esenciales identificados	69
El análisis de riesgos está actualizado al último año	Si
Porcentaje de activos esenciales con un análisis de riesgos actualizado en el último año	100 %
Indique cuándo ha realizado la última actualización	n.a

## 9 ANEXO C. ACTIVIDADES ORGANIZATIVAS

Para valorar las actividades organizativas se utiliza la siguiente escala en tanto por ciento (%).

Porcentaje de avance	Descripción del nivel
%	
0	<i>No se ha iniciado la actividad.</i>
10	<i>La actividad está solamente iniciada.</i>
50	<i>La actividad está a medias.</i>
80	<i>La actividad está muy avanzada.</i>
90	<i>La actividad está prácticamente acabada.</i>
100	<i>La actividad está completa.</i>

Se incluye el valor registrado para las métricas asociadas a las medidas organizativas:

Métrica	Valor Registrado
Roles y Responsabilidades: El responsable de la seguridad es independiente del responsable del sistema	Sí
Política de Seguridad: Se dispone de una política de seguridad aprobada	L3 - La actividad está muy avanzada
Porcentaje de normas de seguridad implantadas	40 %
Porcentaje de procedimientos de seguridad implantados	40 %
Declaración de aplicabilidad: Se dispone de una declaración de aplicabilidad en actualizada	L3 - La actividad está muy avanzada
Plan de adecuación: Se mantiene actualizado el plan de adecuación	L2 - La actividad está a medias

## 10 ANEXO D. RECURSOS

En primer lugar, se presentan los valores registrados en relación a los recursos humanos (equipo de seguridad). Se solicita en INES el número de administradores de seguridad y el número de personas con responsabilidad en la seguridad TIC. Los valores registrados han sido los siguientes:

Equipo de seguridad TIC	Valor Registrado
Número de administradores de seguridad	5
Número de personas con responsabilidad en la STIC	5

En segundo lugar, se presentan los valores asociados a los recursos dedicados a seguridad TIC sobre el total de recursos sobre TIC. Los valores son solicitados como fracción de los recursos destinados a seguridad de las tecnologías de la comunicación e información en el último año sobre el total de recursos dedicados a tecnologías de comunicación e información. Los recursos STIC son aquellos empleados en todas las tareas relacionadas con la seguridad de las TIC. En el valor registrado en INES se han tenido en cuenta las siguientes actividades:

- Tareas técnicas: preventivas y de resolución de incidentes.
- Tareas administrativas; incluyendo contratación de personas, bienes y servicios.
- Tareas de conciencias y formación en materia de seguridad.
- Tareas de comunicación con las autoridades.

Porcentaje de horas destinadas a STIC sobre las dedicadas a TIC	25 %
Porcentaje del presupuesto TIC dedicado a seguridad TIC	30 %

A continuación, se presentan el desglose del presupuesto de seguridad TIC dedicado a:

- Concienciación y formación.
- Subcontratación de personal externo.
- Contratación de servicios de seguridad.
- Adquisición y mantenimiento de productos de STIC.

Desglose del presupuesto	
Fracción del presupuesto STIC dedicado a concienciación y formación	20 %
Fracción del presupuesto STIC dedicado a personal externo	20 %
Fracción del presupuesto STIC dedicado a servicios externos	30 %
Fracción del presupuesto STIC dedicado a adquisición y mantenimiento de productos	30 %

El desglose del presupuesto en STIC debe sumar 100%.

## 11 ANEXO E. INTERCONEXIÓN CON OTROS SISTEMAS

Este apartado es de aplicación a aquellos sistemas de información que se conectan a otros para intercambiar datos y servicios. Todos los aspectos de interconexión de este apartado se centran únicamente en la interconexión con Internet.

<b>Sistema de protección perimetral</b>	
Forma de conexión a Internet	Nos conectamos nosotros directamente
Nombre del organismo a través del cual se conecta a Internet	n.a
Sistema de protección perimetral	APP-5: DMZ con 2 cortafuegos de diferente fabricante + 1 proxy
Madurez del sistema de protección perimetral	L3 - Proceso definido (80%)
<b>Madurez de las herramientas de seguridad</b>	
Herramienta anti-código dañino	L4 - Gestionado y medible (90%)
Análisis de vulnerabilidades	L1 - Inicial/ad hoc (10%)
Análisis de los registros de actividad (logs)	L1 - Inicial/ad hoc (10%)
IDS-IPS. Detección y prevención de intrusión	L4 - Gestionado y medible (90%)
Monitorización de tráfico	L3 - Proceso definido (80%)
Verificación de la configuración	L2 - Reproducible, pero intuitivo (50%)
DLP - Prevención de fuga de datos	L2 - Reproducible, pero intuitivo (50%)
<b>Acceso remoto de equipos portátiles</b>	
Red privada virtual (VPN).	L5 - Optimizado (100%)

## 12 ANEXO F. APLICACIÓN DE LA SEGURIDAD

### IDENTIFICACIÓN Y AUTENTICACIÓN

En este apartado se intenta registrar el uso de los diferentes mecanismos disponibles para acceder al sistema. Se contabilizan los puntos de acceso en los que se requiere la identificación del usuario:

Métrica	Valor Registrado
<b>Usuarios Internos</b>	
Puntos de acceso que emplean usuario/contraseñas	100 %
Puntos de acceso que emplean tarjetas o dispositivos	70 %
Puntos de acceso que emplean biometría	100 %
<b>Usuarios Externo</b>	
Puntos de acceso que emplean usuario/contraseñas	100 %
Puntos de acceso que emplean tarjetas o dispositivos	100 %
Puntos de acceso que emplean claves concertadas	20 %
Puntos de acceso que emplean doble canal	100 %

### SERVICIOS SUBCONTRATADOS

Se definen servicios subcontratados como aquellos proporcionados por terceros, bien sea por medio de contrato o de convenio.

Servicios de ...	Valor Registrado
Comunicaciones	Sí
Acceso a Internet (ISP)	Sí
Alojamiento de servidores	Housing
Alojamiento de servidores - Housing	No
Copias de seguridad	No
Equipamiento hardware de respaldo	No
Instalación de respaldo (centro alternativo)	No
Nube	SaaS, IaaS
Identificación y autenticación	Sí
Firma electrónica	Sí
Sellado de tiempo	Sí
Seguridad gestionada	Sí
Otros	NADA

## **GESTIÓN DE CAMBIOS**

Se ha registrado información sobre el número de veces en el año que se han producido actualizaciones en los distintos servidores, dispositivos de red y equipos de trabajo. Destacando el tiempo que se tarda en aplicar el 50% y el 90% de las actualizaciones y los casos en que estas llevan más de 30 días sin aplicarse al sistema.

De igual forma, por su relevancia, se ha registrado el porcentaje de equipos y dispositivos de red que tiene sistemas operativos fuera de soporte y que, por tanto, no se realiza mantenimiento de seguridad por parte del fabricante.

A continuación, se presentan los valores registrados:

<b>Instalación de actualizaciones (parches) de seguridad en el último año</b>	<b>Frecuencia<sup>2</sup></b>	<b>Porcentaje<sup>3</sup></b>	<b>Madurez<sup>4</sup></b>	<b>T(50)<sup>5</sup></b>	<b>T(90)<sup>6</sup></b>	<b>Sup<sup>7</sup></b>
Sede electrónica / Portal institucional y servidores Web expuestos a Internet	90	100	L2 - Reproducible, pero intuitivo (50%)	7	14	0
En servidores (Web no expuestos a Internet, SQL, Controladores de Dominio, etc...)	90	50	L2 - Reproducible, pero intuitivo (50%)	7	14	0
En equipos de trabajo	7	100	L3 - Proceso definido (80%)	1	1	0
En los dispositivos de electrónica de red (enrutadores, conmutadores, <i>firewalls</i> , etc...)	90	100	L2 - Reproducible, pero intuitivo (50%)	7	14	0
<b>Equipos con sistemas operativos fuera de soporte</b>				<b>Valor Registrado</b>		
Porcentaje de equipos (servidores y estaciones de trabajo) con				10		

2 Frecuencia con la que aplica actualizaciones de seguridad en los equipos de trabajo.

3 Porcentaje de actualizaciones de seguridad aplicadas en los equipos de trabajo, respecto al total que debería haber realizado.

4 Madurez de los mecanismos y procesos que tiene establecidos para la actualización de los equipos de trabajo.

5 Tiempo que se tarda en aplicar el 50% de las actualizaciones.

6 Tiempo que se tarda en aplicar el 90% de las actualizaciones.

7 Número de actualizaciones que llevan más de 30 días sin aplicarse al sistema

sistemas operativos fuera de soporte	
Porcentaje de dispositivos de electrónica de red (enrutadores, conmutadores, <i>firewalls</i> , etc...) cuyo <i>firmware</i> está fuera de soporte.	0

### **CONTINUIDAD DE OPERACIONES**

Se han registrado también valores asociados a indicadores relacionados con la continuidad de operaciones. Los valores registrados en la herramienta INES han sido los siguientes:

Indicadores asociados a la continuidad de operaciones de los activos esenciales de nivel ALTO	Valor Registrado
Porcentaje de activos esenciales de nivel Alto con un análisis de impacto actualizado al último año	0 %
Porcentaje de activos esenciales de nivel Alto con un plan de continuidad actualizado al último año	70 %
Porcentaje de activos esenciales de nivel Alto cuyo plan de continuidad ha sido verificado en el último año	70 %
Número de horas sin servicio (indisponibilidad) en el año de los activos esenciales de nivel Alto	0

### **FORMACIÓN Y CONCIENCIACIÓN**

INES ha solicitado información en relación el esfuerzo realizado tanto en cursos de formación STIC al equipo de seguridad TIC, como a los cursos de formación y sesiones de concienciación STIC dirigidos a toda la organización, incluida la formación a distancia y los cursos online en ambos casos. Los valores registrados son los siguientes:

Formación y Concienciación	Horas
Equipo de seguridad (STIC): Número de horas por persona dedicadas a cursos de <b>formación</b> (incluidos los cursos <i>online</i> ).	50
Usuarios internos: Número de horas por persona empleadas en cursos de formación o sesiones de <b>concienciación</b> (incluida la realizada <i>online</i> ).	3

## 13 ANEXO G. GESTIÓN DE INCIDENTES

La información registrada en INES en relación a la gestión de incidentes incluye únicamente a los incidentes con un impacto significativo. Es decir, aquellos cuyo impacto ha sido clasificado como ALTO, MUY ALTO o CRÍTICO.

El número de incidentes que han sido registrados (propios y los registrados por las sondas del SAT-SARA y SAT-INET) junto con sus tiempos de resolución son recogidos en la siguiente tabla:

Incidentes con impacto ALTO, MUY ALTO o CRÍTICO	Valor registrado
<b>Incidentes de interrupción del servicio (disponibilidad)</b>	
Número de incidentes de nivel CRÍTICO, MUY ALTO y ALTO en el último año.	0
Número de horas en que se han resuelto el 50% de los incidentes de disponibilidad de nivel CRÍTICO, MUY ALTO y ALTO en el último año.	n.a
Número de horas en que se han resuelto el 90% de los incidentes de disponibilidad de nivel CRÍTICO, MUY ALTO y ALTO en el último año.	n.a
Número de incidentes de disponibilidad de nivel CRÍTICO, MUY ALTO y ALTO que llevan más de 36 horas abiertos.	n.a
<b>Resto de incidentes</b>	
Número de incidentes de seguridad de la información de nivel CRÍTICO, MUY ALTO y ALTO en el último año	0
Número de días en que se han resuelto el 50% de los incidentes de seguridad de la información de nivel CRÍTICO, MUY ALTO y ALTO en el último año.	n.a
Número de días en que se han resuelto el 90% de los incidentes de seguridad de la información de nivel CRÍTICO, MUY ALTO y ALTO en el último año.	n.a
Número de incidentes de seguridad de la información de nivel CRÍTICO, MUY ALTO y ALTO que han estado más de 21 días abiertos.	n.a

## 14 ANEXO H. AUDITORÍAS

La información registrada sobre auditorías se divide en cuatro agrupaciones distintas:

- **Auditorías ENS:** Auditorías realizadas para evaluar la adecuación con el ENS (a través de los niveles de madurez de la implantación de las medidas de seguridad).
- **Certificaciones/Conformidades ENS:** Información asociada a la concesión de una certificación de cumplimiento con el ENS (como resultado positivo de una auditoría).
- **Otras auditorías:** Otro tipo de auditorías de seguridad que han podido ser realizadas.
- **Otras certificaciones de seguridad:** Información asociada a la concesión de una certificación de cumplimiento acorde a otros esquemas de seguridad.

Auditorías ENS	Bajo	Medio	Alto
Se dispone de una auditoría de ENS realizada en el último año	No	No	n.a
Número de no conformidades MAYORES encontradas en la última auditoría	n.a	n.a	n.a
Número de no conformidades MENORES encontradas en la última auditoría	n.a	n.a	n.a
Certificaciones / Conformidades de cumplimiento con el ENS	Bajo	Medio	Alto
El sistema disfruta de una certificación o declaración de conformidad en vigor con el ENS	No	No	n.a
Fecha de concesión de la certificación o declaración de conformidad con el ENS	n.a	n.a	n.a
Otras auditorías			
Se dispone de una auditoría técnica o de otro tipo distinto del ENS en vigor	Si		
Indicar las auditorías técnicas o de otro tipo que dispone	Sindicatura de Cuentas		
Número de no conformidades MAYORES encontradas en la última auditoría	0		
Número de no conformidades MENORES encontradas en la última auditoría	15		
Certificaciones / Conformidades de seguridad			
El sistema disfruta de una certificación en vigor de cualquier otro tipo, distinto del ENS. Indicar cual/es y la fecha de concesión de la certificación	n.a		

## 15 INDICADORES CLAVE DE RIESGO (KRI)

Se han registrado los datos asociados a los tres (3) indicadores clave de riesgo: indicador de derechos de usuarios, indicador de dispositivos propios de usuarios y el indicador de rotación de personal.

- **Derecho de los usuarios:** Porcentaje de los equipos cliente de los usuarios internos sobre el total de equipos del sistema en los que la configuración y su gestión están bajo control exclusivo de los técnicos del organismo.
- **Dispositivos propios del usuario:** Porcentaje de personal o trabajadores que emplean dispositivos propios para acceder a los sistemas.
- **Indicador de personal:** Tasa de rotación del personal dedicado a seguridad TIC en el último año.

<b>Derechos de los usuarios</b>	
Porcentaje de los equipos cliente empleados por el personal en los que la configuración y su gestión están bajo control exclusivo de los administradores de seguridad del organismo	100
<b>Derechos de los usuarios</b>	
Porcentaje de equipos que son propiedad del personal (es decir, no de la organización) sobre el total de equipos del sistema, empleados para acceder a los sistemas	0
Porcentaje de los equipos que son propiedad del personal sobre el total de equipos del sistema, en los que la configuración y su gestión están bajo control exclusivo de los administradores de seguridad del organismo	0
<b>Rotación de personal de seguridad TIC</b>	
Número de personas dedicadas a la seguridad TIC que ha causado baja en el último año, aunque se haya podido cubrir la vacante	0

Lugar y fecha:

El Responsable de Seguridad