DIPUTACIÓ DE CASTELLÓ

CCN centro criptológico nacional

INFORME INDIVIDUAL DEL ESTADO DE SEGURIDAD

Diputación de Castellón

ÍNDICE

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 RD 311/2022, de 3 mayo, 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	***Inexistente***. No existe un proceso que soporte el servicio requerido.
L1	***Inicial. Ad hoc***. Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. El resultado es impredecible. Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática..

NIVEL DE MADUREZ	DESCRIPCIÓN DEL NIVEL
Nivel	
L2	***Reproducible, pero intuitivo***. Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos..
L3	***Proceso definido***. Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados de coordinación entre grupos, formación del personal, técnicas de ingeniería, etc.
L4	***Gestionado y medible.*** Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad.
L5	***Optimizado***. La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Figura 1.- Niveles de madurez

CATEGORÍA DEL SISTEMA	NIVEL MÍNIMO DE MADUREZ REQUERIDO
BÁSICA	L2 Reproducible, pero intuitivo
MEDIA	L3 Proceso definido
ALTA	L4 Gestionado y medible

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 realizan las siguientes consideraciones:

- **Perfil ENS (ANEXO II del RD 311/2022).** 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
BÁSICA	L5
MEDIA	L4
ALTA	L0

Figura 4.- Índice de cumplimiento de Diputación de Castellón

	Índice de Cumplimiento
BÁSICA	L3
MEDIA	L2
ALTA	L2

Figura 5.- Mediana global del índice de cumplimiento

	Índice de Cumplimiento
BÁSICA	L3
MEDIA	L2
ALTA	L1

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

El valor objetivo a conseguir es L5.

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	0
MEDIA	0.56
ALTA	100

Figura 7.- Índice de mejora de Diputación de Castellón

	Índice de Mejora
BÁSICA	10.87
MEDIA	36.33
ALTA	40.2

Figura 8.- Mediana global del índice de mejora

	Índice de Mejora
BÁSICA	11.17
MEDIA	41.17
ALTA	58.85

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

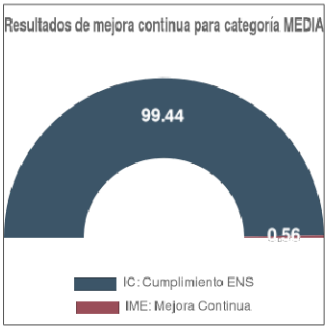

Figura 11.- Resultados de Mejora Continua para categoría MEDIA

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	L3
MEDIA	L3
ALTA	L0

Figura 13.- Índice de madurez de Diputación de Castellón

	Índice de Madurez
BÁSICA	L2
MEDIA	L2
ALTA	L2

Figura 14.- Mediana global del índice de madurez

	Índice de Madurez
BÁSICA	L2
MEDIA	L1
ALTA	L1

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 60.

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	Bajo	Medio	n.a
Nivel de la Integridad	Bajo	Medio	n.a
Nivel de la Trazabilidad	Bajo	Bajo	n.a
Nivel de la Autenticidad	Bajo	Bajo	n.a
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 73 medidas del Esquema Nacional de Seguridad:

[ORG] MARCO ORGANIZATIVO

Marco organizativo		Madurez o n.a.		
[Org]	Medidas	BÁSICA	MEDIA	ALTA
[org.1]	Política de seguridad	L3 - Proceso definido	L3 - Proceso definido	n.a
[org.2]	Normativa de seguridad	L3 - Proceso definido	L3 - Proceso definido	n.a
[org.3]	Procedimientos de seguridad	L3 - Proceso definido	L3 - Proceso definido	n.a
[org.4]	Proceso de autorización	L3 - Proceso definido	L3 - Proceso definido	n.a

[OP] MARCO OPERACIONAL

Marco operacional		Madurez o n.a.		
[Op]	Medidas	BÁSICA	MEDIA	ALTA
[op.pl]	**Planificación**	**L3 - Proceso definido**	**L2 - Reproducible, pero intuitivo**	**L0 - Inexistente**
[op.pl.1]	Análisis de riesgos	L4 - Gestionado y medible	L4 - Gestionado y medible	n.a
[op.pl.2]	Arquitectura de seguridad	L3 - Proceso definido	L3 - Proceso definido	n.a

Marco operacional		Madurez o n.a.		
[Op]	Medidas	BÁSICA	MEDIA	ALTA
[op.pl.3]	Adquisición de nuevos componentes	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.pl.4]	Dimensionamiento/gestión de la capacidad	L3 - Proceso definido	L2 - Reproducible, pero intuitivo	n.a
[op.pl.5]	Componentes certificados	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.acc]	**Control de acceso**	**L3 - Proceso definido**	**L3 - Proceso definido**	**L0 - Inexistente**
[op.acc.1]	Identificación	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.acc.2]	Requisitos de acceso	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.acc.3]	Segregación de funciones y tareas	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.acc.4]	Proceso de gestión de derechos de acceso	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.acc.5]	Mecanismo de autenticación (usuarios externos)	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.acc.6]	Mecanismo de autenticación (usuarios de la organización)	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.exp]	**Explotación**	**L3 - Proceso definido**	**L3 - Proceso definido**	**L0 - Inexistente**
[op.exp.1]	Inventario de activos	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.exp.2]	Configuración de seguridad	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.exp.3]	Gestión de la configuración de seguridad	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.exp.4]	Mantenimiento y actualizaciones de seguridad	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.exp.5]	Gestión de cambios	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.exp.6]	Protección frente a código dañino	L3 - Proceso definido	L3 - Proceso definido	n.a

Marco operacional		Madurez o n.a.		
[Op]	Medidas	BÁSICA	MEDIA	ALTA
[op.exp.7]	Gestión de incidentes	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.exp.8]	Registro de la actividad	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.exp.9]	Registro de la gestión de incidentes	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.exp.10]	Protección de claves criptográficas	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.ext]	**Recursos externos**	**L3 - Proceso definido**	**L3 - Proceso definido**	**L0 - Inexistente**
[op.ext.1]	Contratación y acuerdos de nivel de servicio	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.ext.2]	Gestión diaria	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.ext.3]	Protección de la cadena de suministro	No aplica	No aplica	n.a
[op.ext.4]	Interconexión de sistemas	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.nub]	**Servicios en la nube**	**L3 - Proceso definido**	**L3 - Proceso definido**	**L0 - Inexistente**
[op.nub.1]	Protección de servicios en la nube	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.cont]	**Continuidad del servicio**	**L3 - Proceso definido**	**L3 - Proceso definido**	**L0 - Inexistente**
[op.cont.1]	Análisis de impacto	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.cont.2]	Plan de continuidad	No aplica	No aplica	n.a
[op.cont.3]	Pruebas periódicas	No aplica	No aplica	n.a
[op.cont.4]	Medios alternativos	No aplica	No aplica	n.a
[op.mon]	**Monitorización del sistema**	**L3 - Proceso definido**	**L3 - Proceso definido**	**L0 - Inexistente**
[op.mon.1]	Detección de intrusión	L3 - Proceso definido	L3 - Proceso definido	n.a

Marco operacional		Madurez o n.a.		
[Op]	Medidas	BÁSICA	MEDIA	ALTA
[op.mon.2]	Sistema de métricas	L3 - Proceso definido	L3 - Proceso definido	n.a
[op.mon.3]	Vigilancia	L3 - Proceso definido	L3 - Proceso definido	n.a

[MP] MEDIDAS DE PROTECCIÓN

Medidas de protección		Madurez o n.a.		
[mp]	Medidas	BÁSICA	MEDIA	ALTA
[mp.if]	**Protección de las instalaciones e infraestructuras**	**L4 - Gestionado y medible**	**L4 - Gestionado y medible**	**L0 - Inexistente**
[mp.if.1]	Áreas separadas y con control de acceso	L5 - Optimizado	L5 - Optimizado	n.a
[mp.if.2]	Identificación de las personas	L4 - Gestionado y medible	L4 - Gestionado y medible	n.a
[mp.if.3]	Acondicionamiento de los locales	L4 - Gestionado y medible	L4 - Gestionado y medible	n.a
[mp.if.4]	Energía eléctrica	L4 - Gestionado y medible	L4 - Gestionado y medible	n.a
[mp.if.5]	Protección frente a incendios	L4 - Gestionado y medible	L4 - Gestionado y medible	n.a
[mp.if.6]	Protección frente a inundaciones	L4 - Gestionado y medible	L4 - Gestionado y medible	n.a
[mp.if.7]	Registro de entrada y salida de equipamiento	L5 - Optimizado	L5 - Optimizado	n.a

Medidas de protección		Madurez o n.a.		
[mp]	Medidas	BÁSICA	MEDIA	ALTA
[mp.per]	**Gestión del personal**	**L3 - Proceso definido**	**L3 - Proceso definido**	**L0 - Inexistente**
[mp.per.1]	Caracterización del puesto de trabajo	No aplica	L3 - Proceso definido	n.a
[mp.per.2]	Deberes y obligaciones	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.per.3]	Concienciación	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.per.4]	Formación	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.eq]	**Protección de los equipos**	**L3 - Proceso definido**	**L3 - Proceso definido**	**L0 - Inexistente**
[mp.eq.1]	Puesto de trabajo despejado	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.eq.2]	Bloqueo de puesto de trabajo	No aplica	L3 - Proceso definido	n.a
[mp.eq.3]	Protección de equipos portátiles	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.eq.4]	Otros dispositivos conectados a la red	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.com]	**Protección de las comunicaciones**	**L3 - Proceso definido**	**L3 - Proceso definido**	**L0 - Inexistente**
[mp.com.1]	Perímetro seguro	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.com.2]	Protección de la confidencialidad	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.com.3]	Protección de la integridad y de la autenticidad	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.com.4]	Separación de flujos de información en la red	No aplica	L3 - Proceso definido	n.a
[mp.si]	**Protección de los soportes de información**	**L3 - Proceso definido**	**L3 - Proceso definido**	**L0 - Inexistente**
[mp.si.1]	Marcado de soportes	No aplica	L3 - Proceso definido	n.a

Medidas de protección		Madurez o n.a.		
[mp]	Medidas	BÁSICA	MEDIA	ALTA
[mp.si.2]	Criptografía	No aplica	L3 - Proceso definido	n.a
[mp.si.3]	Custodia	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.si.4]	Transporte	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.si.5]	Borrado y destrucción	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.sw]	**Protección de las aplicaciones informáticas**	**L3 - Proceso definido**	**L3 - Proceso definido**	**L0 - Inexistente**
[mp.sw.1]	Desarrollo de aplicaciones	No aplica	L3 - Proceso definido	n.a
[mp.sw.2]	Aceptación y puesta en servicio	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.info]	**Protección de la información**	**L3 - Proceso definido**	**L3 - Proceso definido**	**L0 - Inexistente**
[mp.info.1]	Datos personales	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.info.2]	Calificación de la información	No aplica	L3 - Proceso definido	n.a
[mp.info.3]	Firma electrónica	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.info.4]	Sellos de tiempo	No aplica	No aplica	n.a
[mp.info.5]	Limpieza de documentos	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.info.6]	Copias de seguridad	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.s]	**Protección de los servicios**	**L3 - Proceso definido**	**L3 - Proceso definido**	**L0 - Inexistente**
[mp.s.1]	Protección del correo electrónico	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.s.2]	Protección de servicios y aplicaciones web	L3 - Proceso definido	L3 - Proceso definido	n.a
[mp.s.3]	Protección frente a la denegación de servicio	L3 - Proceso definido	L3 - Proceso definido	n.a

Medidas de protección		Madurez o n.a.		
[mp]	Medidas	BÁSICA	MEDIA	ALTA
[mp.s.4]	Protección frente a la denegación de servicio	No aplica	L3 - Proceso definido	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
Proceso de autorización [org.4]	L3 - Proceso definido	L3 - Proceso definido	n.a
Análisis de riesgos [op.pl.1]	L4 - Gestionado y medible	L4 - Gestionado y medible	n.a
Proceso de gestión de derechos de acceso [op.acc.4]	L3 - Proceso definido	L3 - Proceso definido	n.a
Gestión de incidentes [op.exp.7]	L3 - Proceso definido	L3 - Proceso definido	n.a
Concienciación y Formación [mp.per.3 + mp.per.4]	L3 - Proceso definido	L3 - Proceso definido	n.a
Configuración de seguridad y gestión de cambios [op.exp.4 + op.exp.5]	L3 - Proceso definido	L3 - Proceso definido	n.a
Continuidad de operaciones [op.cont.1 + op.cont.2 + op.cont.3 + op.cont.4 + mp.info.6]	L3 - Proceso definido	L3 - Proceso definido	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	200
Número de activos esenciales identificados	30
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	*No se ha iniciado la actividad.*
10	*La actividad está solamente iniciada.*
50	*La actividad está a medias.*
80	*La actividad está muy avanzada.*
90	*La actividad está prácticamente acabada.*
100	*La actividad está completa.*

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	60 %
Porcentaje de procedimientos de seguridad implantados	60 %
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	L3 - La actividad está muy avanzada

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	6
Número de personas con responsabilidad en la STIC	8

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	40 %
Porcentaje del presupuesto TIC dedicado a seguridad TIC	50 %

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	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.

Sistema de protección perimetral	
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
Madurez del sistema de protección perimetral	L3 - Proceso definido
Madurez de las herramientas de seguridad	
Herramienta anti-código dañino	L4 - Gestionado y medible
Análisis de vulnerabilidades	L3 - Proceso definido
Análisis de los registros de actividad (logs)	L3 - Proceso definido
IDS-IPS. Detección y prevención de intrusión	L4 - Gestionado y medible
Monitorización de tráfico	L3 - Proceso definido
Verificación de la configuración	L2 - Reproducible, pero intuitivo
DLP Prevención de fuga de datos	L2 - Reproducible, pero intuitivo
Acceso remoto de equipos portátiles	
Red privada virtual (VPN).	L5 - Optimizado

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
Usuarios Internos	
Puntos de acceso que emplean usuario/contraseñas	100 %
Puntos de acceso que emplean tarjetas o dispositivos	70 %
Puntos de acceso que emplean biometría	0 %
Usuarios Externo	
Puntos de acceso que emplean usuario/contraseñas	100 %
Puntos de acceso que emplean tarjetas o dispositivos	100 %
Puntos de acceso que emplean claves concertadas	0 %
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	No
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:

Instalación de actualizaciones (parches) de seguridad en el último año	Frecuencia	Porcentaje	Madurez	T(50)	T(90)	Sup
Sede electrónica / Portal institucional y servidores Web expuestos a Internet	30	100	L3 - Proceso definido	7	14	0
En servidores (Web no expuestos a Internet, SQL, Controladores de Dominio, etc…)	30	80	L3 - Proceso definido	7	14	0
En equipos de trabajo	30	100	L3 - Proceso definido	1	1	0
En los dispositivos de electrónica de red (enrutadores, conmutadores, *firewalls*, etc…)	90	100	L2 - Reproducible, pero intuitivo	7	14	0

Equipos con sistemas operativos fuera de soporte	Valor Registrado
Porcentaje de equipos (servidores y estaciones de trabajo) con sistemas operativos fuera de soporte	10
Porcentaje de dispositivos de electrónica de red (enrutadores, conmutadores, *firewalls*, etc…) cuyo *firmware* 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	100 %
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 **formación** (incluidos los cursos *online*).	50
Usuarios internos: Número de horas por persona empleadas en cursos de formación o sesiones de **concienciación** (incluida la realizada *online*).	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
Incidentes de interrupción del servicio (disponibilidad)	
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
Resto de incidentes	
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	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	No		
Indicar las auditorías técnicas o de otro tipo que	n.a		
Número de no conformidades MAYORES encontradas en la última auditoría	n.a		
Número de no conformidades MENORES encontradas en la última auditoría	n.a		
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.

Derechos de los usuarios	
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
Derechos de los usuarios	
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	0
Rotación de personal de seguridad TIC	
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