DIPUTACIÓN DE ALMERÍA

CCN centro criptológico nacional

INFORME INDIVIDUAL DEL ESTADO DE SEGURIDAD 2019

Diputación de Almería

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 a lo previsto 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.

2. FINALIDAD

Se prevé recopilar esta información anualmente sobre un amplio espectro del sector público español y no solo de las Administraciones públicas como hasta ahora, de forma que podamos al cabo de unos años ver la evolución del país, y que cada organismo pueda 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).

Con el informe INES del organismo se busca:

- una estimación preventiva de la seguridad, vía análisis del cumplimiento de determinados aspectos que se han estimado críticos para cualquier organismo.
- una estimación de la eficacia y eficiencia de las actividades llevadas a cabo en materia de seguridad.
- una estimación del esfuerzo humano y económico dedicado a seguridad TIC.

3. METODOLOGÍA

Para la recogida de datos de este informe se ha empleado la herramienta INES (Informe Nacional del Estado de Seguridad) basada en los establecido en la actualizada guía CCN-STIC-824 Informe del Estado de Seguridad. La herramienta INES se encuentra en operación desde 2014, y permite la carga de datos de acuerdo al Anexo II del Esquema Nacional de Seguridad, tanto de forma automática como manual.

Paran facilitar la carga automática de datos, se puede recurrir a las herramientas PILAR (de análisis y gestión de riesgos), LUCÍA (de gestión de ciberincidentes) y otras, que incorporan mecanismos para recopilar y exportar los indicadores que les competan, facilitando la recopilación de datos solicitados en INES. PILAR se basa en la metodología MAGERIT[1] y existe una versión reducida, denominada microPILAR (μPILAR), para facilitar el trabajo de los organismos que disponen de sistemas más elementales.

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

1 Magerit Versión 3: Metodología de Análisis y Gestión de Riesgos de los sistemas de Información. Consejo Superior de Administración Electrónica.

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	***Inexistente***. Esta salvaguarda no existe en este momento.
L1	10	***Inicial/ad hoc***. Se hace cuando se considera adecuado, pero no está establecido.
L2	50	***Reproducible, pero intuitivo***. Se realiza, pero no está formalizado documentalmente.
L3	80	***Proceso definido***. Se realiza y está definido documentalmente (procedimientos).
L4	90	***Gestionado y medible.*** Se están gestionando y son susceptibles de ser medidas.
L5	100	***Optimizado***. 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

Umbrales de madurez de la categoría de un sistema.

Categoría del Sistema	Rojo Inferior	Amarillo Inferior	Nivel Adecuado
BÁSICA	≤ 40%	≤ 50%	>50% (L2 o superior)
MEDIA	≤ 70%	≤ 80%	>80% (L3 o superior)
ALTA	≤ 80%	≤ 90	>90% (L4 o superior)

Figura 3.- Umbrales de madurez del sistema

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 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 4.- 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.

4. PARTICIPACIÓN

El número de organismos que han registrado datos en INES dentro de su agrupación (Diputación o cabildo) es de 55.

El número de sistemas es el siguiente:

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

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

Dimensión	Valor Registrado		
	BÁSICA	MEDIA	ALTA

Dimensión	Valor Registrado		
	BÁSICA	MEDIA	ALTA
Nivel de la Confidencialidad	n.a	Medio	n.a
Nivel de la Integridad	n.a	Medio	n.a
Nivel de la Disponibilidad	n.a	Medio	n.a
Nivel de la Autenticidad	n.a	Medio	n.a
Nivel de la Trazabilidad	n.a	Medio	n.a

5. MEDIDAS DEL ANEXO II DEL ENS

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

Marco organizativo		Madurez o n.a.[2]		
[Org]	Medidas	BÁSICA	MEDIA	ALTA
[org.1]	Política de seguridad	n.a	10	n.a
[org.2]	Normativa de seguridad	n.a	10	n.a
[org.3]	Procedimientos de seguridad	n.a	0	n.a
[org.4]	Proceso de autorización	n.a	10	n.a

Marco operacional		Madurez o n.a.		
[Op]	Medidas	BÁSICA	MEDIA	ALTA
[op.pl]	**Planificación**	**n.a**	**24.00**	**n.a**
[op.pl.1]	Análisis de riesgos	n.a	80	n.a

2 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.pl.2]	Arquitectura de seguridad	n.a	0	n.a
[op.pl.3]	Adquisición de nuevos componentes	n.a	0	n.a
[op.pl.4]	Dimensionamiento / Gestión de capacidades	n.a	40	n.a
[op.pl.5]	Componentes certificados	n.a	0	n.a
[op.acc]	**Control de acceso**	**n.a**	**33.57**	**n.a**
[op.acc.1]	Identificación	n.a	50	n.a
[op.acc.2]	Requisitos de acceso	n.a	50	n.a
[op.acc.3]	Segregación de funciones y tareas	n.a	10	n.a
[op.acc.4]	Proceso de gestión de derechos de acceso	n.a	50	n.a
[op.acc.5]	Mecanismo de autenticación	n.a	50	n.a
[op.acc.6]	Acceso local	n.a	0	n.a
[op.acc.7]	Acceso remoto	n.a	25	n.a
[op.exp]	**Explotación**	**n.a**	**3.45**	**n.a**
[op.exp.1]	Inventario de activos	n.a	0	n.a
[op.exp.2]	Configuración de seguridad	n.a	10	n.a
[op.exp.3]	Gestión de la configuración	n.a	8	n.a
[op.exp.4]	Mantenimiento	n.a	10	n.a
[op.exp.5]	Gestión de cambios	n.a	10	n.a
[op.exp.6]	Protección frente a código dañino	n.a	0	n.a
[op.exp.7]	Gestión de incidentes	n.a	0	n.a
[op.exp.8]	Registro de la actividad de los usuarios	n.a	0	n.a
[op.exp.9]	Registro de la gestión de incidentes	n.a	0	n.a
[op.exp.10]	Protección de los registros de actividad	n.a	0	n.a
[op.exp.11]	Protección de claves criptográficas	n.a	0	n.a
[op.ext]	**Servicios externos**	**n.a**	**3.33**	**n.a**
[op.ext.1]	Contratación y acuerdos de nivel de	n.a	10	n.a

Marco operacional		Madurez o n.a.		
[Op]	Medidas	BÁSICA	MEDIA	ALTA
	servicio			
[op.ext.2]	Gestión diaria	n.a	0	n.a
[op.ext.9]	Medios alternativos	n.a	0	n.a
[op.cont]	**Continuidad del servicio**	**n.a**	**0.00**	**n.a**
[op.cont.1]	Análisis de impacto	n.a	0	n.a
[op.cont.2]	Plan de continuidad	n.a	0	n.a
[op.cont.3]	Pruebas periódicas	n.a	0	n.a
[op.mon]	**Monitorización del sistema**	**n.a**	**60.00**	**n.a**
[op.mon.1]	Detección de intrusión	n.a	80	n.a
[op.mon.2]	Sistema de métricas	n.a	40	n.a

Medidas de protección		Madurez o n.a.		
[mp]	Medidas	BÁSICA	MEDIA	ALTA
[mp.if]	**Protección de las instalaciones e infraestructuras**	**n.a**	**45.00**	**n.a**
[mp.if.1]	Áreas separadas y con control de acceso	n.a	10	n.a
[mp.if.2]	Identificación de las personas	n.a	50	n.a
[mp.if.3]	Acondicionamiento de los locales	n.a	80	n.a
[mp.if.4]	Energía eléctrica	n.a	80	n.a
[mp.if.5]	Protección frente a incendios	n.a	80	n.a
[mp.if.6]	Protección frente a inundaciones	n.a	50	n.a
[mp.if.7]	Registro de entrada y salida de equipamiento	n.a	10	n.a
[mp.if.9]	Instalaciones alternativas	n.a	0	n.a
[mp.per]	**Gestión del personal**	**n.a**	**4.00**	**n.a**
[mp.per.1]	Caracterización del puesto de trabajo	n.a	80	n.a

Medidas de protección		Madurez o n.a.		
[mp]	Medidas	BÁSICA	MEDIA	ALTA
[mp.per.2]	Deberes y obligaciones	n.a	0	n.a
[mp.per.3]	Concienciación	n.a	10	n.a
[mp.per.4]	Formación	n.a	10	n.a
[mp.per.9]	Personal alternativo	n.a	0	n.a
[mp.eq]	**Protección de los equipos**	**n.a**	**40.00**	**n.a**
[mp.eq.1]	Puesto de trabajo despejado	n.a	0	n.a
[mp.eq.2]	Bloqueo de puesto de trabajo	n.a	80	n.a
[mp.eq.3]	Protección de equipos portátiles	n.a	0	n.a
[mp.eq.9]	Medios alternativos	n.a	80	n.a
[mp.com]	**Protección de las comunicaciones**	**n.a**	**34.60**	**n.a**
[mp.com.1]	Perímetro seguro	n.a	50	n.a
[mp.com.2]	Protección de la confidencialidad	n.a	80	n.a
[mp.com.3]	Protección de la autenticidad y de la integridad	n.a	43	n.a
[mp.com.4]	Segregación de redes	n.a	0	n.a
[mp.com.9]	Medios alternativos	n.a	0	n.a
[mp.si]	**Protección de los soportes de información**	**n.a**	**34.00**	**n.a**
[mp.si.1]	Etiquetado	n.a	50	n.a
[mp.si.2]	Criptografía	n.a	10	n.a
[mp.si.3]	Custodia	n.a	10	n.a
[mp.si.4]	Transporte	n.a	50	n.a
[mp.si.5]	Borrado y destrucción	n.a	50	n.a
[mp.sw]	**Protección de las aplicaciones informáticas**	**n.a**	**10.00**	**n.a**
[mp.sw.1]	Desarrollo	n.a	10	n.a
[mp.sw.2]	Aceptación y puesta en servicio	n.a	10	n.a
[mp.info]	**Protección de la información**	**n.a**	**17.14**	**n.a**

Medidas de protección		Madurez o n.a.		
[mp]	Medidas	BÁSICA	MEDIA	ALTA
[mp.info.1]	Datos de carácter personal	n.a	50	n.a
[mp.info.2]	Calificación de la información	n.a	0	n.a
[mp.info.3]	Cifrado	n.a	0	n.a
[mp.info.4]	Firma electrónica	n.a	10	n.a
[mp.info.5]	Sellos de tiempo	n.a	10	n.a
[mp.info.6]	Limpieza de documentos	n.a	0	n.a
[mp.info.9]	Copias de seguridad *(backup)*	n.a	50	n.a
[mp.s]	**Protección de los servicios**	**n.a**	**27.50**	**90.00**
[mp.s.1]	Protección del correo electrónico	n.a	50	n.a
[mp.s.2]	Protección de servicios y aplicaciones web	n.a	10	n.a
[mp.s.8]	Protección frente a la denegación de servicio	n.a	50	n.a
[mp.s.9]	Medios alternativos	n.a	0	n.a

6. 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	
Dispone de AR en lenguaje natural, realizado como exposición textual	
Dispone de AR semiformal, usando lenguaje específico y presentación con tablas	
Dispone de AR formal, usando lenguaje específico y con metodología reconocida internacionalmente	
Número de activos totales en el análisis de riesgos	122
Número de activos esenciales identificados	34
El análisis de riesgos está actualizado al último año	Si

Análisis y Gestión de Riesgos	Valor Registrado
Porcentaje de activos esenciales con un análisis de riesgos actualizado en el último año	0 %
Indique cuándo ha realizado la última actualización	n.a

7. 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.*

Figura 5.- Escala de valoración de las actividades organizativas

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	L0 - No se ha iniciado la actividad
Porcentaje de normas de seguridad implantadas	0 %
Porcentaje de procedimientos de seguridad implantados	0 %
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

8. 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	4
Número de personas con responsabilidad en la STIC	4

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	4 %

Umbrales: Cada organismo puede comprobar su ubicación en la siguiente escala de rangos, donde se indican los umbrales verde, amarillo y rojo, inferior y superior, para cada categoría de sistema.

Categoría	< 1%	1% - 2%	2% - 4%	4% - 8%	8% - 16%	> 16%
BÁSICA						
MEDIA						
ALTA						

Figura 6.- Umbrales del porcentaje de recursos dedicados a la STIC respecto a los dedicados a las TIC

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	0 %

Fracción del presupuesto STIC dedicado a personal externo	0 %
Fracción del presupuesto STIC dedicado a servicios externos	10 %
Fracción del presupuesto STIC dedicado a adquisición y mantenimiento de productos	90 %

El desglose del presupuesto en STIC debe sumar 100%.

9. 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 proxy
Madurez del sistema de protección perimetral	L2 - Reproducible, pero intuitivo (50%)
Madurez de las herramientas de seguridad	
Herramienta anti-código dañino	L2 - Reproducible, pero intuitivo (50%)
Análisis de vulnerabilidades	L2 - Reproducible, pero intuitivo (50%)
Análisis de los registros de actividad (logs)	L0 - Inexistente (0%)
IDS-IPS. Detección y prevención de intrusión	L2 - Reproducible, pero intuitivo (50%)
Monitorización de tráfico	L2 - Reproducible, pero intuitivo (50%)
Verificación de la configuración	L1 - Inicial/ad hoc (10%)
DLP - Prevención de fuga de datos	L1 - Inicial/ad hoc (10%)
Acceso remoto de equipos portátiles	
Red privada virtual (VPN).	L2 - Reproducible, pero intuitivo (50%)

10. APLICACIÓN DE LA SEGURIDAD

10.1 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	99 %
Puntos de acceso que emplean tarjetas o dispositivos	20 %
Puntos de acceso que emplean biometría	2 %
Usuarios Externo	
Puntos de acceso que emplean usuario/contraseñas	100 %
Puntos de acceso que emplean tarjetas o dispositivos	20 %
Puntos de acceso que emplean claves concertadas	0 %
Puntos de acceso que emplean doble canal	0 %

10.2 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	n.a
Alojamiento de servidores - Housing	No
Copias de seguridad	No
Equipamiento hardware de respaldo	No
Instalación de respaldo (centro alternativo)	No
Nube	PaaS
Identificación y autenticación	Sí
Firma electrónica	Sí
Sellado de tiempo	Sí

Servicios de …	Valor Registrado
Seguridad gestionada	No
Otros	

10.3 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[3]	Porcentaje[4]	Madurez[5]	T(50)[6]	T(90)[7]	Sup[8]
Sede electrónica / Portal institucional y servidores Web expuestos a Internet			No definido	1	1	0
En servidores (Web no expuestos a Internet, SQL, Controladores de Dominio, etc…)			No definido	1	1	0
En equipos de trabajo			No definido	1	1	0
En los dispositivos de electrónica de red (enrutadores, conmutadores, *firewalls*, etc…)			No definido	0	0	10
Equipos con sistemas operativos fuera de soporte						

[3] Frecuencia con la que aplica actualizaciones de seguridad en los equipos de trabajo.

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

[5] Madurez de los mecanismos y procesos que tiene establecidos para la actualización de los equipos de trabajo.

[6] Tiempo que se tarda en aplicar el 50% de las actualizaciones.

[7] Tiempo que se tarda en aplicar el 90% de las actualizaciones.

[8] Número de actualizaciones que llevan más de 30 días sin aplicarse al sistema

Porcentaje de equipos (servidores y estaciones de trabajo) con sistemas operativos fuera de soporte	40
Porcentaje de dispositivos de electrónica de red (enrutadores, conmutadores, *firewalls*, etc…) cuyo *firmware* está fuera de soporte.	80

Umbrales: Días que se tarda en aplicar las diferentes actualizaciones teniendo en cuenta que aquellas consideradas críticas se aplicarán tan pronto como sea posible.

Actualizaciones en	T(50)			T(90)		
	verde	amarillo	rojo	verde	amarillo	rojo
Sede Electrónica	< 5 d	> 5 d	> 14 d	< 7 d	> 7 d	> 21 d
Resto servidores	< 15 d	> 15 d	> 30 d	< 20 d	> 20 d	> 40 d
Equipos de trabajo	< 10 d	> 10 d	> 21 d	< 12 d	> 12 d	> 25 d
Electrónica de red	< 15 d	> 15 d	> 30 d	< 20 d	> 20 d	> 40 d

Figura 7.- Gestión de actualizaciones (parches) de seguridad. Umbrales de aplicación en días

10.4 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	0 %
Porcentaje de activos esenciales de nivel Alto cuyo plan de continuidad ha sido verificado en el último año	0 %
Número de horas sin servicio (indisponibilidad) en el año de los activos esenciales de nivel Alto	0

10.5 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

Formación y Concienciación	Horas
Equipo de seguridad (STIC): Número de horas por persona dedicadas a cursos de **formación** (incluidos los cursos *online*).	0
Usuarios internos: Número de horas por persona empleadas en cursos de formación o sesiones de **concienciación** (incluida la realizada *online*).	5

11. 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 abiertos.	n.a

Umbrales de interrupción del servicio (disponibilidad): horas que se tarda en cubrir el porcentaje de incidentes significativos (alto/ muy alto / crítico) cerrados, relativos a interrupción del servicio (disponibilidad).

T(50)			T(90)		
verde	amarillo	rojo	verde	amarillo	rojo
< 24h	> 24h	> 48h	< 36h	> 36h	> 48h

Figura 8.- Gestión de incidentes. Umbrales de interrupción del servicio en horas

Umbrales del resto de clases de incidentes: días que se tarda en cubrir el porcentaje de incidentes significativos (alto/ muy alto / crítico) cerrados, relativos al resto de clases de incidentes distintos a los de interrupción del servicio (disponibilidad).

T(50)			T(90)		
Verde	Amarillo	Rojo	Verde	Amarillo	Rojo
< 4d	> 4d	> 14d	< 5d	> 5d	> 18d

Figura 9.- Gestión de incidentes. Umbrales del resto de clases de incidentes en días

12. 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	n.a	Si	n.a
Número de no conformidades MAYORES encontradas en la última auditoría	n.a		n.a
Número de no conformidades MENORES encontradas en la última auditoría	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	n.a	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 dispone	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			

13. 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	95
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	1
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
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

14. 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]	n.a	10	n.a
Análisis de riesgos [op.pl.1]	n.a	80	n.a
Gestión de derechos de acceso [op.acc.4]	n.a	50	n.a
Gestión de incidentes [op.exp.7]	n.a	0	n.a
Concienciación y Formación [mp.per.3 + mp.per.4]	n.a	10	n.a
Configuración de seguridad y gestión de cambios [op.exp.4 + op.exp.5]	n.a	10	n.a
Continuidad de operaciones [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]	n.a	13	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.

15. INDICADORES AGREGADOS

15.1 ORGANIZACIÓN DE LA SEGURIDAD

El indicador agregado asociado a la organización de la seguridad viene determinado por la combinación de los valores registrados para los siguientes aspectos individuales:

- Política de Seguridad
- Independencia entre responsable del sistema y de seguridad
- Análisis de riesgos actualizados
- Declaración de aplicabilidad actualizada
- Plan de seguridad ENS actualizado
- Declaración o certificación de conformidad actualizado
- Normas de seguridad implantadas
- Procedimientos de seguridad implantados

El valor agregado para Diputación de Almería es:

- Categoría BÁSICA: 0.00
- Categoría MEDIA: 0.00
- Categoría ALTA: 0.00

El valor objetivo a conseguir es del **100.** Si se dispone de una declaración o certificación de conformidad con el ENS en vigor el indicador será 100.

15.2 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.

El índice de madurez de Diputación de Almería es:

- Categoría BÁSICA 0.00.
- Categoría MEDIA 23.55.
- Categoría ALTA 0.00.

Mediana global del índice de madurez:

- Categoría BÁSICA 47.23.
- Categoría MEDIA 54.75.
- Categoría ALTA 58.09.

Mediana global del índice de madurez para su ámbito:

- Categoría BÁSICA 52.94.
- Categoría MEDIA 46.84.
- Categoría ALTA 51.64.

El nivel que se debe, como mínimo, alcanzar, para los sistemas de las distintas categorías es:

- Categoría BÁSICA: 50%
- Categoría MEDIA: 80%
- Categoría ALTA: 90%

Sin embargo, lo recomendado es conseguir **100%**.

Se definen los siguientes umbrales y colores:

Categoría	Rojo	Amarillo	Adecuado
BÁSICA	≤ 40	≤ 50	> 50
MEDIA	≤ 70	≤ 80	> 80
ALTA	≤ 80	≤ 90	> 90

Figura 10.- Umbrales y colores asociados al Índice de Madurez

Los datos de los valores generales del Índice de Madurez, tanto globales como los correspondientes al ámbito, no serán definitivos hasta que la campaña de recogida de datos no haya finalizado.

15.3 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 Almería es:

- Categoría BÁSICA: 0.00.
- Categoría MEDIA: 34.84.
- Categoría ALTA: 0.00.

Mediana global del índice de cumplimiento:

- Categoría BÁSICA 84.
- Categoría MEDIA 67.56.
- Categoría ALTA 63.43.

Mediana global del índice de cumplimiento para su ámbito:

- Categoría BÁSICA 83.89.
- Categoría MEDIA 59.28.
- Categoría ALTA 57.38.

El valor objetivo a conseguir es de **100%.**

Se definen los siguientes umbrales y colores correspondientes al Índice de cumplimiento (valores ajustados). Esta tabla se aplicará a todos los sistemas independientemente de su categoría. El objetivo es obtener 100% o 100 puntos.

Categorías	Rojo	Amarillo	Adecuado
Todas las categorías de sistema	< 87	< 97	> 97

Figura 11.- Umbrales y colores asociados al Índice de Cumplimiento

Los datos de los valores generales de Índice de Cumplimiento, tanto globales como los correspondientes al ámbito, no serán definitivos hasta que la campaña de recogida de datos no haya finalizado.

16. CONCLUSIONES

Durante 2019 se ha trabajado en la consolidación la organización de la Seguridad de la Información, para ello el Comité de Seguridad de la Información se ha reunión de forma periódica y se han ido dando directrices y aprobando actuaciones para garantizar la Organización de la Seguridad.

El ritmo para la implantación es lento pero continuo, intentando concienciar a toda la Organización en la Seguridad de la Información, para ello se han realizado reuniones y cursos de formación.

Para avanzar más rápidamente y debido a la escasez de recursos, en 2019 la Diputación de Almería ha adjudicado a empresa INGENIA el apoyo para la adecuación al ENS, a través de una oficina técnica que acompañara durante 2 o 3 años para la adecuación y la certificación en el ENS.

Somos conscientes que para prestar unos servicios electrónico de garantía es necesario disponer de una buena organización e implantación de la Seguridad de la Información, y para ello estamos trabajando para una Certificación al ENS en el corto o medio plazo.

17. PROPUESTAS DE MEJORA

Como propuesta de mejora para avanzar en la implantación del ENS y de la Seguridad de la Información, se proponen para 2020, las siguientes:

- Redactar y aprobar Política de Seguridad y Privacidad.
- Elaboran y aprobar Plan de adecuación al ENS
- Elaborar y aprobar el plan de aplicabilidad de las medidas de seguridad.
- Elaborar y aprobar un plan detallado de Mejora, con los proyectos y subproyectos a ralizar.
- Elaborar y aprobar Normas.
- Elaborar y aprobar Procedimientos.
- Elaborar y aprobar guías y recomendaciones.
- Implantación de las Medidas de seguridad.
- Diseñar acciones formativas para concienciación y difusión Seguridad de Información.

Lugar y fecha:
Almería

El Responsable de Seguridad
Jefe de Servicio de Organización e Información