GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

CCN
CENTRO CRIPTOLÓGICO NACIONAL

GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-824)

ESQUEMA NACIONAL DE SEGURIDAD

INFORME DEL ESTADO DE SEGURIDAD (BORRADOR)

ens
Esquema Nacional de Seguridad

NOVIEMBRE 2014

Edita:

NIPO: 002-14-030-X

Fecha de Edición: noviembre de 2014

El Sr. José Antonio Mañas ha elaborado el presente documento y sus anexos.
El Ministerio de Hacienda y Administraciones Públicas ha financiado el desarrollo del presente documento y sus anexos.

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 crea del Esquema Nacional de Seguridad (ENS), que establece las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

El Real Decreto 3/2010 de 8 de Enero desarrolla el Esquema Nacional de Seguridad y fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración. En su artículo 29 se autoriza que a través de la series CCN-STIC el CCN desarrolle lo establecido en el mismo.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función y a lo reflejado en el ENS, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Noviembre 2014

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. El Esquema Nacional de Seguridad (ENS) exige evaluar regularmente el estado de seguridad de los sistemas de información:

> Artículo 35. Informe del estado de la seguridad.
> El Comité Sectorial de Administración Electrónica articulará los procedimientos necesarios para conocer regularmente el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere el presente real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones públicas.

2. Así mismo, el ENS exige establecer un sistema de medición de la seguridad del sistema:

> Anexo II – Medidas de seguridad
> 4 Marco operacional [op]
> 4.6 Monitorización del sistema [op.mon]
> 4.6.2 Sistema de métricas [op.mon.2]

dimensiones	todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

> Categoría ALTA
> Se establecerá un conjunto de indicadores que mida el desempeño real del sistema en materia de seguridad, en los siguientes aspectos:
> a) Grado de implantación de las medidas de seguridad.
> b) Eficacia y eficiencia de las medidas de seguridad.
> c) Impacto de los incidentes de seguridad.

3. Este documento describe una serie de medidas e indicadores con 2 destinatarios:
   1. el propio organismo propietario del sistema de información
   2. el informe anual del estado de seguridad de la administración pública española
4. En ambos casos 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
5. Para algunos indicadores se marcan
   - líneas amarillas que detectan una deficiencia leve, un problema potencial que debe estudiarse antes de que sea grave
   - líneas rojas que detectan una deficiencia grave que debe corregirse a la mayor brevedad posible
6. Se prevé recopilar esta información anualmente sobre un amplio espectro de la administración pública española 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

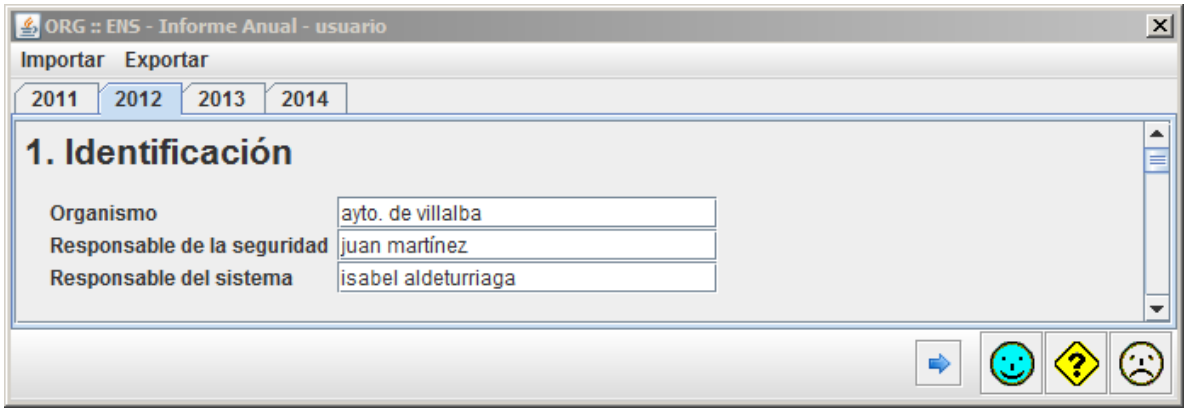
la media nacional. A tal fin, la herramienta PILAR de análisis y gestión de riesgos incorporará mecanismos para recopilar y reportar estos indicadores.

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

2. INFORME ANUAL

8. Se describen los datos que se recopilarán para ser informados anualmente.

2.1 IDENTIFICACIÓN



etiqueta	org
descripción	nombre del organismo
tipo	texto
valores	texto libre

etiqueta	rseg
descripción	responsable de la seguridad
tipo	texto
valores	texto libre

etiqueta	rsis
descripción	responsable del sistema
tipo	texto
valores	texto libre

2.2 ORGANIZACIÓN DE LA SEGURIDAD

2.2.1 ACTIVIDADES

9. LL Se analizan varias actividades organizativas, estableciéndose una escala cualitativa de valoración en 5 niveles. A saber:

1	no se ha iniciado la actividad
2	la actividad está solamente iniciada
3	la actividad está en curso
4	está prácticamente completada

5	actividad completada

etiqueta	b_policy
descripción	se dispone de una política de seguridad aprobada
tipo	entero
valores	rango 1-5
objetivo	5

etiqueta	rseg-rsis
descripción	el responsable de la seguridad es independiente del responsable del sistema
tipo	entero
valores	rango 1-5
objetivo	5

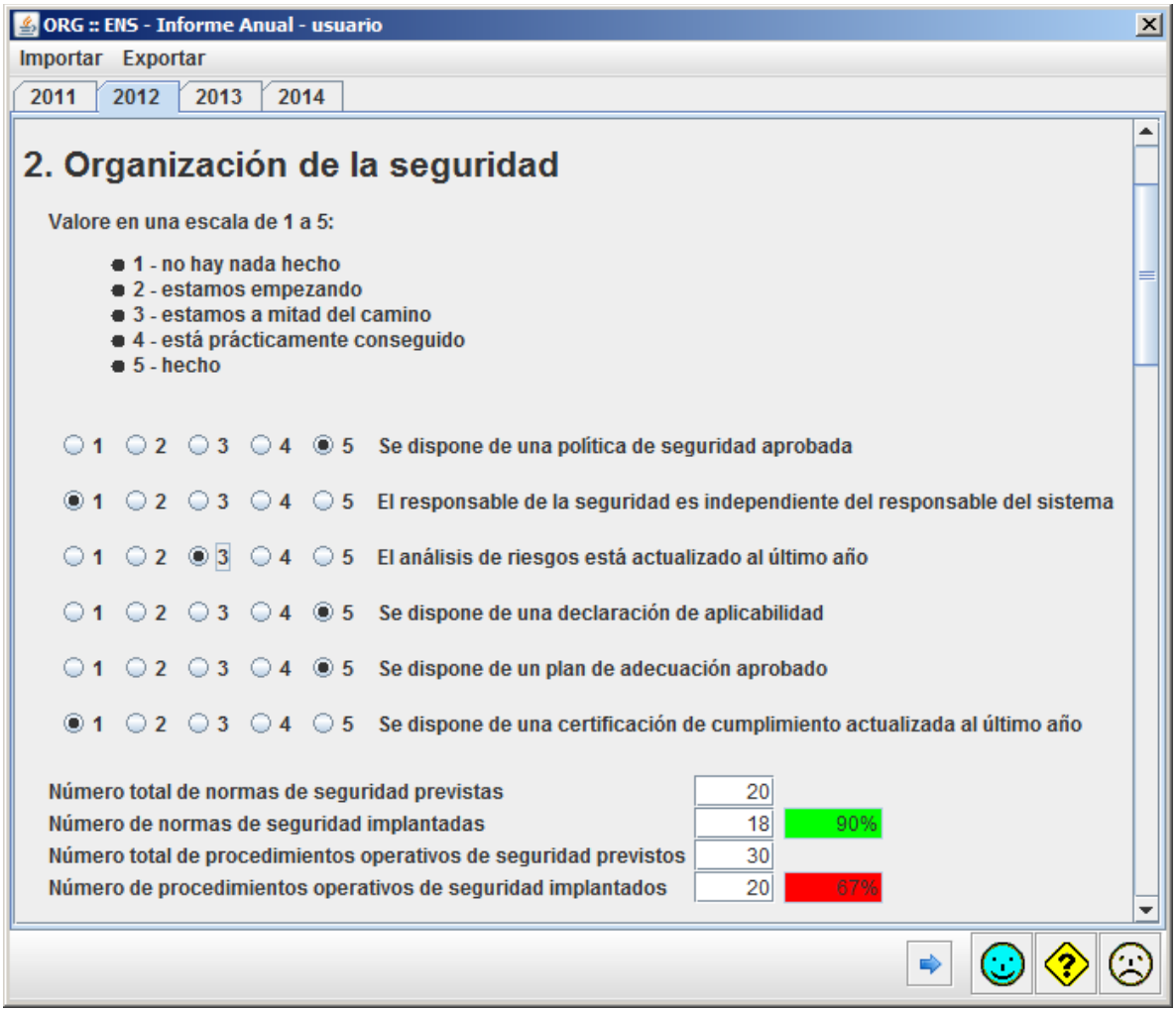
etiqueta	b_risk
descripción	el análisis de riesgos está actualizado al último año
tipo	entero
valores	rango 1-5
objetivo	5

etiqueta	b_soa
descripción	se dispone de una declaración de aplicabilidad
tipo	entero
valores	rango 1-5
objetivo	5

etiqueta	b_plan
descripción	se dispone de un plan de adecuación aprobado
tipo	entero
valores	rango 1-5
objetivo	5

etiqueta	b_cert
descripción	se dispone de una certificación de cumplimiento actualizada al último año
tipo	entero
valores	rango 1-5
objetivo	5

10. Se adjunta un ejemplo tomado de la herramienta PILAR:



2.2.2 NORMATIVA Y PROCEDIMIENTOS DE SEGURIDAD

etiqueta	policies.total
descripción	número total de normas de seguridad previstas
tipo	entero
valores	> 0

etiqueta	policies.current
descripción	número de normas de seguridad implantadas
tipo	entero
valores	0 .. policies.total
objetivo	policies.total

etiqueta	policies.p
descripción	porcentaje de normas de seguridad implantadas
tipo	porcentaje
fórmula	policies.current / policies.total
valores	0% .. 100%
objetivo	100%

11. Umbrales: Porcentaje de normas de seguridad implantadas

categoría	rojo inferior	amarillo inferior	amarillo superior	rojo superior
ALTA	50%	80%	n.a.	n.a.
MEDIA	33%	70%	n.a.	n.a.
BAJA	25%	60%	n.a.	n.a.

etiqueta	pos.total
descripción	número total de procedimientos operativos de seguridad previstas
tipo	entero
valores	> 0

etiqueta	pos.current
descripción	número de procedimientos operativos de seguridad implantadas
tipo	entero
valores	0 .. pos.total
objetivo	pos.total

etiqueta	pos.p
descripción	porcentaje de procedimientos operativos de seguridad implantadas
tipo	porcentaje
fórmula	pos.current / pos.total
valores	0% .. 100%
objetivo	100%

12. Umbrales: Porcentaje de procedimientos operativos de seguridad implantados

categoría	rojo inferior	amarillo inferior	amarillo superior	rojo superior
ALTA	75%	95%	n.a.	n.a.
MEDIA	50%	66%	n.a.	n.a.
BAJA	n.a.	33%	n.a.	n.a.

2.3 IDENTIFICACIÓN Y AUTENTICACIÓN

13. Se trata de inventariar el uso de los diferentes mecanismos disponibles.

2.3.1 INTERNA

14. Mecanismo de autenticación para personal interno (trabajadores del organismo, propios o subcontratados)

etiqueta	ia.int.password
descripción	sistemas que emplean contraseñas
tipo	porcentaje
valores	0% .. 100%

etiqueta	ia.int.token
descripción	sistemas que emplean tokens
tipo	porcentaje
valores	0% .. 100%

etiqueta	ia.int.bio
descripción	sistemas que emplean biometría
tipo	porcentaje
valores	0% .. 100%

2.3.2 EXTERNA

15. Mecanismo de autenticación para usuarios externos: administrados que no son personal del organismo

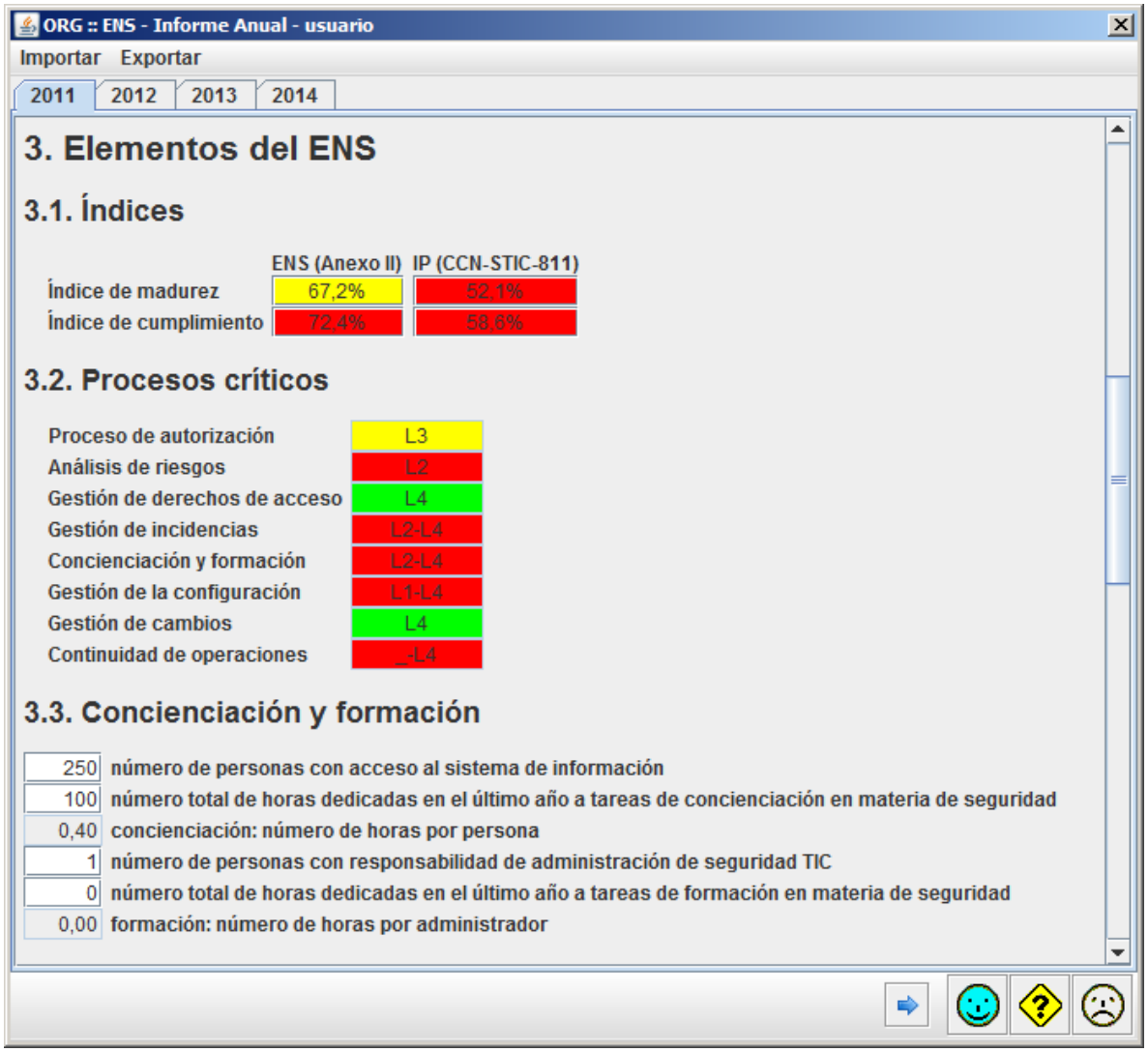
etiqueta	ia.ext.password
descripción	sistemas que emplean contraseñas
tipo	porcentaje
valores	0% .. 100%

etiqueta	ia.ext.cc
descripción	sistemas que emplean claves concertadas
tipo	porcentaje
valores	0% .. 100%

etiqueta	ia.ext.token
descripción	sistemas que emplean tokens (ej. DNI electrónico)
tipo	porcentaje
valores	0% .. 100%

etiqueta	ia.ext.2
descripción	sistemas que emplean doble canal (ej. contraseñas de un solo uso sobre SMS)
tipo	porcentaje
valores	0% .. 100%

2.4 ELEMENTOS DEL ENS



2.4.1 ÍNDICES

etiqueta	index.maturity.ens
descripción	Índice de madurez del ENS (Anexo II)
tipo	porcentaje
valores	0% .. 100%
objetivo	por categoría

etiqueta	index.compliance.ens
descripción	Índice de cumplimiento del ENS (Anexo II)
tipo	porcentaje
valores	0% .. 100%
objetivo	100%

etiqueta	index.maturity.ip
descripción	Índice de madurez de la interconexión (CCN-STIC.811)
tipo	porcentaje
valores	0% .. 100%
objetivo	por categoría

etiqueta	index.compliance.ip
descripción	Índice de madurez de la interconexión (CCN-STIC.811)
tipo	porcentaje
valores	0% .. 100%
objetivo	100%

16. Umbrales: Índices de madurez

categoría	rojo inferior	amarillo inferior	amarillo superior	rojo superior
ALTA	66%	80%	n.a.	n.a.
MEDIA	50%	66%	n.a.	n.a.
BAJA	20%	33%	n.a.	n.a.

17. Umbrales: Índices de cumplimiento

categoría	rojo inferior	amarillo inferior	amarillo superior	rojo superior
ALTA	75%	95%	n.a.	n.a.
MEDIA	50%	66%	n.a.	n.a.
BAJA	50%	66%	n.a.	n.a.

2.4.2 PROCESOS CRÍTICOS

Proceso	**madurez**
Proceso de autorización [org.4]	
Análisis de riesgos [op.pl.1]	
Gestión de derechos de acceso [op.acc.4]	
Gestión de incidentes [op.exp.7]	
Concienciación y formación [mp.per.3 + mp.per.4]	
Configuración de seguridad [op.exp.2] + Gestión de la configuración [op.exp.3]	
Mantenimiento [op.exp.4] + Gestión de cambios [op.exp.5]	
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]	

categoría	rojo inferior	amarillo inferior	objetivo
ALTA	L2	L3	L4
MEDIA	L1	L2	L3
BAJA	L0	L1	L2

2.4.3 PROCESO DE AUTORIZACIÓN [ORG.4]

18. Indicadores de eficacia.
19. Se mide el número de incidentes debidos a fallos del proceso de autorización.

etiqueta	process.org-4.n_high
descripción	número de incidentes de nivel ALTO debidos a fallos del proceso de autorización
tipo	entero
valores	≥ 0
objetivo	0

etiqueta	process.org-4.n_medium
descripción	número de incidentes de nivel MEDIO debidos a fallos del proceso de autorización
tipo	entero
valores	≥ 0
objetivo	0

etiqueta	process.org-4.p_high
descripción	número de incidentes de nivel ALTO por usuario debidos a fallos del proceso de autorización
tipo	porcentaje
fórmula	process.org-4.n_high / users.total
valores	0% .. 100%
objetivo	0%

etiqueta	process.org-4.p_medium
descripción	número de incidentes de nivel MEDIO por usuario debidos a fallos del proceso de autorización
tipo	porcentaje
	process.org-4.n_medium / users.total
valores	0% .. 100%
objetivo	0%

2.4.4 ANÁLISIS DE RIESGOS [OP.PL.1]

20. Indicadores predictivos, de implantación.

etiqueta	assets.essential.total
descripción	número de activos esenciales
tipo	entero
valores	> 0

etiqueta	process.op-pl-1.n
descripción	número de elementos esenciales con un análisis de riesgos actualizado en el último año
tipo	entero
valores	0 .. assets.essential.total
objetivo	assets.essential.total

etiqueta	process.op-pl-1.p
descripción	proporción de elementos esenciales con un análisis de riesgos actualizado en el último año
tipo	porcentaje
fórmula	process.op-pl-1.n / assets.essential.total
valores	0% .. 100%
objetivo	1000%

2.4.5 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO [OP.ACC.4]

21. Indicadores de eficacia.
22. Se mide el número de incidentes debidos a fallos del proceso de gestión de derechos de acceso.

etiqueta	process.op-acc-4.n_high
descripción	número de incidentes de nivel ALTO debidos a fallos del proceso de gestión de derechos de acceso
tipo	entero
valores	≥ 0
objetivo	0

etiqueta	process.op-acc-4.n_medium
descripción	número de incidentes de nivel MEDIO debidos a fallos del proceso de gestión de derechos de acceso
tipo	entero
valores	≥ 0
objetivo	0

etiqueta	process.op-acc-4.p_high
descripción	número de incidentes de nivel ALTO por usuario debidos a fallos del proceso de gestión de derechos de acceso
tipo	porcentaje
fórmula	process.op-acc-4.n_high / users.total
valores	0% .. 100%
objetivo	0%

etiqueta	process.op-acc-4.p_medium
descripción	número de incidentes de nivel MEDIO por usuario debidos a fallos del proceso de gestión de derechos de acceso
tipo	porcentaje
fórmula	process.op-acc-4.n_medium / users.total
valores	0% .. 100%
objetivo	0%

2.4.6 CONFIGURACIÓN DE SEGURIDAD

23. Indicadores relativos a las medidas de protección [op.exp.2] y [op.exp.3]
24. Indicadores de eficacia.
25. Se mide el número de incidentes debidos a fallos del proceso de establecimiento y mantenimiento de la configuración de seguridad.

etiqueta	process.op-exp-2.n_high
descripción	número de incidentes de nivel ALTO debidos a fallos del proceso de establecimiento y mantenimiento de la configuración de seguridad
tipo	entero
valores	≥ 0
objetivo	0

etiqueta	process.op-exp-2.n_medium
descripción	número de incidentes de nivel MEDIO debidos a fallos del proceso de establecimiento y mantenimiento de la configuración de seguridad
tipo	entero
valores	≥ 0
objetivo	0

etiqueta	process.op-exp-2.p_high
descripción	número de incidentes de nivel ALTO por usuario debidos a fallos del proceso de establecimiento y mantenimiento de la configuración de seguridad
tipo	porcentaje
fórmula	process.op-exp-2.n_high / users.total
valores	0% .. 100%
objetivo	0%

etiqueta	process.op-exp-2.p_medium
descripción	número de incidentes de nivel MEDIO por usuario debidos a fallos del proceso de establecimiento y mantenimiento de la configuración de seguridad
tipo	porcentaje
fórmula	process.op-exp-2.n_medium / users.total
valores	0% .. 100%
objetivo	0%

2.4.7 GESTIÓN DE CAMBIOS

26. Indicadores relativos a las medidas de protección [op.exp.4] y [op.exp.5]

2.4.7.1 INDICADORES DE IMPLANTACIÓN.

etiqueta	process.op-exp-4.t50_high
descripción	tiempo que se tarda en actualizar el 50% del software desde que se anuncia una actualización hasta que se ha aplicado; activos de nivel ALTO
tipo	real
valores	días
objetivo	0

etiqueta	process.op-exp-4.t90_high
descripción	tiempo que se tarda en actualizar el 90% del software desde que se anuncia una actualización hasta que se ha aplicado; activos de nivel ALTO
tipo	real
valores	días
objetivo	process.op-exp-4.t50_high

etiqueta	process.op-exp-4.s30_high
descripción	activos de nivel ALTO que llevan más de 30 días pendientes de que se aplique una actualización
tipo	entero
valores	≥ 0
objetivo	0

etiqueta	process.op-exp-4.t50_medium
descripción	tiempo que se tarda en actualizar el 50% del software desde que se anuncia una actualización hasta que se ha aplicado; activos de nivel MEDIO
tipo	real
valores	días
objetivo	0

etiqueta	process.op-exp-4.t90_medium
descripción	tiempo que se tarda en actualizar el 90% del software desde que se anuncia una actualización hasta que se ha aplicado; activos de nivel MEDIO
tipo	real
valores	días
objetivo	process.op-exp-4.t50_medium

etiqueta	process.op-exp-4.s30_medium
descripción	activos de nivel MEDIO que llevan más de 30 días pendientes de que se aplique una actualización
tipo	entero
valores	≥ 0
objetivo	0

2.4.7.2 INDICADORES DE EFICACIA

27. Se mide el número de incidentes debidos a fallos del proceso de mantenimiento y gestión de cambios.

etiqueta	process.op-exp-4.n_high
descripción	número de incidentes de nivel ALTO debidos a fallos del proceso de mantenimiento y gestión de cambios
tipo	entero
valores	≥ 0
objetivo	0

etiqueta	process.op-exp-4.n_medium
descripción	número de incidentes de nivel MEDIO debidos a fallos del proceso de mantenimiento y gestión de cambios
tipo	entero
valores	≥ 0
objetivo	0

etiqueta	process.op-exp-4.p_high
descripción	número de incidentes de nivel ALTO por usuario debidos a fallos del proceso de mantenimiento y gestión de cambios
tipo	porcentaje
fórmula	process.op-exp-4.n_high / users.total
valores	0% .. 100%
objetivo	0%

etiqueta	process.op-exp-4.p_medium
descripción	número de incidentes de nivel MEDIO por usuario debidos a fallos del proceso de mantenimiento y gestión de cambios
tipo	porcentaje
fórmula	process.op-exp-4.n_medium / users.total
valores	0% .. 100%
objetivo	0%

2.4.8 CONTINUIDAD DE OPERACIONES

28. Indicadores relativos a las medidas de protección [op.cont.*] y [mp.*.9]

2.4.8.1 INDICADORES PREDICTIVOS, DE IMPLANTACIÓN.

etiqueta	process.op-cont.bia_high
descripción	porcentaje de servicios esenciales de nivel ALTO con un análisis de impacto actualizado al último año
tipo	porcentaje
valores	0% .. 100%
objetivo	100%

etiqueta	process.op-cont.drp_high
descripción	porcentaje de servicios esenciales de nivel ALTO con un plan de continuidad actualizado al último año
tipo	porcentaje
valores	0% .. 100%
objetivo	100%

etiqueta	process.op-cont.test_high
descripción	porcentaje de servicios esenciales de nivel ALTO que han sido testados en el último año
tipo	porcentaje
valores	0% .. 100%
objetivo	100%

2.4.8.2 INDICADORES DE EFICACIA

etiqueta	process.op-cont.hours
descripción	horas sin servicio en el último año
tipo	real
valores	horas
objetivo	0

2.4.9 CONCIENCIACIÓN Y FORMACIÓN

29. Indicadores predictivos.

etiqueta	aw.np
descripción	número de personas con acceso al sistema de información
tipo	real
valores	≥ 0

etiqueta	aw.nh
descripción	número total de horas dedicadas en el último año a tareas de concienciación en materia de seguridad
tipo	real
valores	≥ 0

etiqueta	aw.nhp
descripción	concienciación: número de horas por persona
tipo	real
fórmula	aw.nh / aw.np
valores	≥ 0

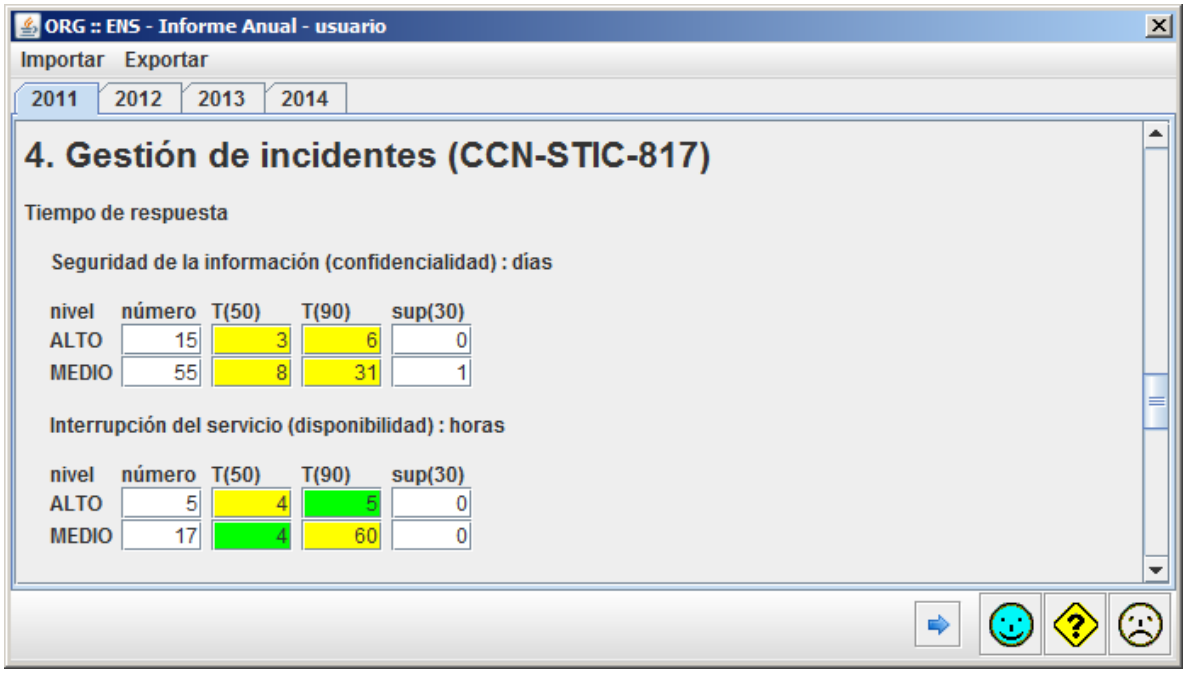
etiqueta	train.np
descripción	número de personas con responsabilidad de administración de seguridad TIC
tipo	real
valores	≥ 0

etiqueta	train.nh
descripción	número total de horas dedicadas en el último año a tareas de formación en materia de seguridad
tipo	real
valores	≥ 0

etiqueta	train.nhp
descripción	número de horas dedicadas a formación del personal en materia de seguridad, dividido por el número de personas dedicadas a la seguridad
tipo	real
fórmula	train.nh / train.np
valores	≥ 0

30. Tasas bajas de concienciación y formación pueden llevar a un esfuerzo propio en la materia, o a la utilización de recursos centrales de concienciación y formación.

2.5 GESTIÓN DE INCIDENTES



31. Indicadores de eficacia.

32. De los incidentes de seguridad se mide el nivel. Ver glosario, Guía CCN-STIC-815, "criticality level (of a security event)". Se usan los niveles definidos en el Anexo I del ENS.

2.5.1 TIEMPO DE RESPUESTA (DÍAS) A LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (CONFIDENCIALIDAD)

etiqueta	incidents.i.n_high
descripción	Número de incidentes de seguridad de la información de nivel ALTO en el último año.
tipo	entero
valores	≥ 0

etiqueta	incidents.i.t50_high
descripción	Número de días en que se han resuelto el 50% de los incidentes de seguridad de la información de nivel ALTO en el último año.
tipo	entero
valores	días

etiqueta	incidents.i.t90_high
descripción	Número de días en que se han resuelto el 90% de los incidentes de seguridad de la información de nivel ALTO en el último año.
tipo	entero
valores	días

etiqueta	incidents.i.s30_high
descripción	Número de incidentes de seguridad de la información de nivel ALTO que llevan más de 30 días abiertos
tipo	entero
valores	≥ 0

etiqueta	incidents.i.n_medium
descripción	Número de incidentes de seguridad de la información de nivel MEDIO en el último año.
tipo	entero
valores	≥ 0

etiqueta	incidents.i.t50_medium
descripción	Número de días en que se han resuelto el 50% de los incidentes de seguridad de la información de nivel MEDIO en el último año.
tipo	entero
valores	días

etiqueta	incidents.i.t90_medium
descripción	Número de días en que se han resuelto el 90% de los incidentes de seguridad de la información de nivel MEDIO en el último año.
tipo	entero
valores	días

etiqueta	incidents.i.s30_medium
descripción	Número de incidentes de seguridad de la información de nivel MEDIO que llevan más de 30 días abiertos
tipo	entero
valores	≥ 0

nivel del impacto	número	T(50)	T(90)	Sup30
ALTO	#	días	días	#
MEDIO	#	días	días	#
BAJO	#	días	días	#

33. Umbrales: días que se tarda en cubrir el porcentaje de incidentes cerrados, relativos a seguridad de la información (confidencialidad)

	T(50)		T(90)	
nivel del impacto	amarillo superior	rojo superior	amarillo superior	rojo superior
ALTO	2d	5d	5d	30d
MEDIO	7d	30d	30d	90d
BAJO	15d	60d	60d	180d

2.5.2 TIEMPO DE RESPUESTA (HORAS) A LOS INCIDENTES DE INTERRUPCIÓN DEL SERVICIO (DISPONIBILIDAD)

etiqueta	incidents.d.n_high
descripción	Número de incidentes de disponibilidad de nivel ALTO en el último año.
tipo	entero
valores	≥ 0

etiqueta	incidents.d.t50_high
descripción	Número de horas en que se han resuelto el 50% de los incidentes de disponibilidad de nivel ALTO en el último año.
tipo	entero
valores	horas

etiqueta	incidents.d.t90_high
descripción	Número de horas en que se han resuelto el 90% de los incidentes de disponibilidad de nivel ALTO en el último año.
tipo	entero
valores	horas

etiqueta	incidents.d.s30_high
descripción	Número de incidentes de seguridad de disponibilidad de nivel ALTO que llevan más de 24 horas abiertos
tipo	entero
valores	≥ 0

etiqueta	incidents.d.n_medium
descripción	Número de incidentes de disponibilidad de nivel MEDIO en el último año.
tipo	entero
valores	≥ 0

etiqueta	incidents.d.t50_medium
descripción	Número de horas en que se han resuelto el 50% de los incidentes de disponibilidad de nivel MEDIO en el último año.
tipo	entero
valores	horas

etiqueta	incidents.d.t90_medium
descripción	Número de horas en que se han resuelto el 90% de los incidentes de disponibilidad de nivel MEDIO en el último año.
tipo	entero
valores	horas

etiqueta	incidents.d.s30_medium
descripción	Número de incidentes de disponibilidad de nivel MEDIO que llevan más de 24 horas abiertos
tipo	entero
valores	≥ 0

nivel del impacto	número	T(50)	T(90)	Sup30
ALTO	#	horas	horas	#
MEDIO	#	horas	horas	#
BAJO	#	horas	horas	#

34. Umbrales: horas que se tarda en cubrir el porcentaje de incidentes cerrados, relativos a interrupción del servicio (disponibilidad)

	T(50)		T(90)	
nivel del impacto	amarillo superior	rojo superior	amarillo superior	rojo superior
ALTA	2h	5h	5h	30h
MEDIA	7h	30h	30h	180h
BAJA	15h	60h	60h	365h

35. Los niveles de madurez nos indican la calidad de las actividades desarrolladas para gestionar la seguridad, son indicadores predictivos, pues una baja madurez de los mismos denota una debilidad de cara a enfrentarnos a incidentes.

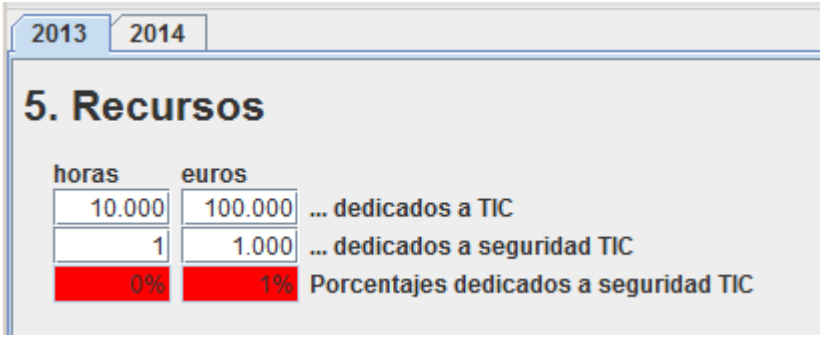
36. En cambio, los incidentes nos muestran la eficacia conseguida. El número de incidentes es un poco relativo, pues no depende tanto de nosotros como de la parte atacante y, además puede haber diferentes criterios para clasificar un incidente de forma individualizada o fragmentada en componentes. En cambio, los tiempos de respuesta son indicativos de la ventana de oportunidad que le cedemos al atacante.

37. Lo idóneo es cerrar todos los incidentes con presteza, aunque se mide el T(90) para no engañarnos con incidentes insidiosos aislados.

38. Si T(90) es alto, es indicación clara de que hay que mejorar el proceso de gestión de incidentes, quizás necesitemos más medios.

39. Si T(50) es claramente inferior a T(90) puede que nos encontremos con un sistema poco profesionalizado pues si el sistema de gestión está bien dotado y bien procedimentado, T(50) debe ser cercano a T(90). En estos casos debemos poner énfasis en elaborar procedimientos que hagan el proceso sistemático.

2.6 RECURSOS



2.6.1 HORAS

etiqueta	tic_h
descripción	Horas dedicadas a TIC
tipo	real
valores	horas

etiqueta	stic_h
descripción	Horas dedicadas a seguridad TIC
tipo	real
valores	horas

etiqueta	p_stic_h
descripción	Porcentaje de horas dedicadas a seguridad TIC sobre el total de horas dedicadas a TIC.
tipo	porcentaje
fórmula	stic_h / tic_h
valores	0% .. 100%

2.6.2 EUROS

etiqueta	tic_e
descripción	Euros dedicados a TIC
tipo	real
valores	euros

etiqueta	stic_e
descripción	Euros dedicados a seguridad TIC
tipo	real
valores	euros

etiqueta	p_stic_e
descripción	Porcentaje de euros dedicados a seguridad TIC sobre el total de euros dedicadas a TIC.
tipo	porcentaje
	stic_e / tic_e
valores	0% .. 100%

40. Medidas e indicadores.

horas	euros	
		(1) dedicados a TIC
		(2) dedicados a seguridad TIC
%	%	(2/1) porcentajes dedicados a seguridad TIC

41. Son datos anuales, bien porque son estables a lo largo del año, bien sumando los datos de cada periodo. No cabe esperar una precisión superior al ±10%.

42. Dedicación TIC incluye todas las tareas relacionadas con Tecnologías de la Información y Comunicaciones:

- tareas técnicas
- tareas administrativas, incluyendo contratación de personas, bienes y servicios.
- tareas docentes (formación)

43. Dedicación STIC incluye todas las tareas relacionadas con la Seguridad de las TIC. Pueden usarse las tareas a las que hace mención el ENS como inventario:

- tareas técnicas: preventivas y de resolución de incidentes
- tareas administrativas, incluyendo contratación de personas, bienes y servicios
- tareas de concienciación y formación
- tareas de comunicación con las autoridades

44. No se hará distinciones en función de la categoría de la persona. Suma lo mismo personal fijo o temporal, propio, desplazado o subcontratado. Cuando se subcontraten servicios, se imputará la carga de trabajo indicada en el contrato de prestación de servicios.

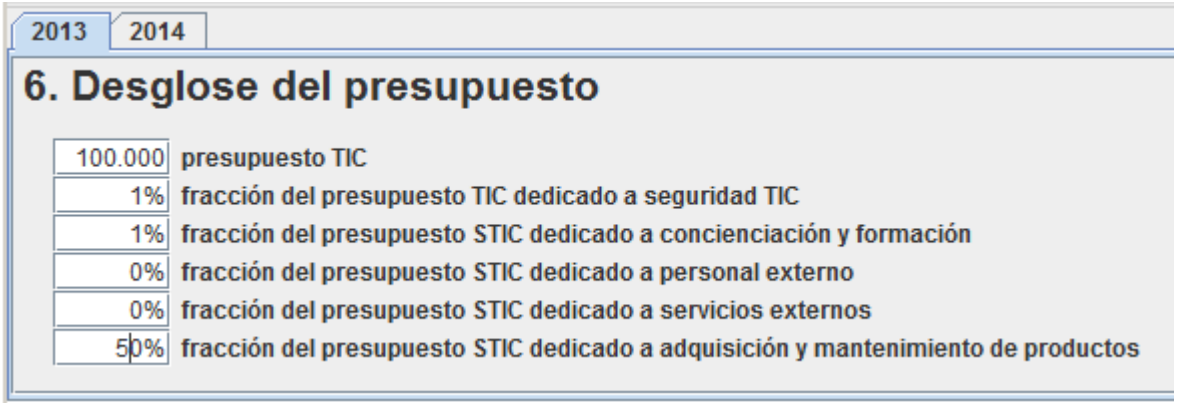
45. Umbrales: porcentajes dedicados a seguridad TIC. Se establece un objetivo y unos umbrales de desviación:

categoría	rojo inferior 50%	amarillo inferior 66%	objetivo	amarillo superior 150%	rojo superior 200%
ALTA	5%	6,5%	10%	15%	20%
MEDIA	2,5%	3%	5%	7,5%	10%
BAJA	1,5%	2%	3%	4,5%	6%

46. Estos indicadores son predictivos. Una deficiencia de recursos es una invitación a tener problemas y dificultades para solucionar los incidentes. No obstante hay aún poca información de dónde deben estar las líneas amarillas y rojas. Probablemente los umbrales haya que revisarlos según vayamos teniendo más datos.

47. En todo caso deben usarse para que los organismos busquen recursos (o reubiquen los recursos disponibles) en caso de debilidad.

2.7 DESGLOSE DEL PRESUPUESTO



48. Medidas e indicadores. Este apartado desglosa los datos económicos recogidos en el apartado anterior.

etiqueta	budget.tic
descripción	Presupuesto TIC.
tipo	real
valores	euros

etiqueta	budget.stic_p
descripción	fracción del presupuesto TIC dedicado a seguridad TIC
tipo	porcentaje
valores	0% .. 100%

etiqueta	budget.stic_aw_p
descripción	fracción del presupuesto STIC dedicado a concienciación y formación
tipo	porcentaje
valores	0% .. 100%

etiqueta	budget.stic_ext_per_p
descripción	fracción del presupuesto STIC dedicado a personal externo
tipo	porcentaje
valores	0% .. 100%

etiqueta	budget.stic_ext_s_p
descripción	fracción del presupuesto STIC dedicado a servicios externos
tipo	porcentaje
valores	0% .. 100%

etiqueta	budget.stic_ext_eq_p
descripción	fracción del presupuesto STIC dedicado a adquisición y mantenimiento de productos
tipo	porcentaje
valores	0% .. 100%

49. Son datos anuales, bien porque son estables a lo largo del año, bien promediando los datos de cada periodo. No cabe esperar una precisión superior al ±10%.

50. Presupuesto TIC incluye todo el gasto relacionado con Tecnologías de la Información y Comunicaciones:

- personal propio (en la proporción que se dedica a TIC)
- contratación de personas, bienes y servicios.
- tareas docentes (formación)

51. Presupuesto STIC incluye la parte del gasto TIC relacionado con la Seguridad de las TIC. Pueden usarse los elementos a los que hace mención el ENS como inventario:

- técnicos: tareas preventivas y de resolución de incidentes
- contratación de personas, bienes y servicios
- gasto en concienciación y formación

52. No se hará distinciones en función de la categoría de la persona. Suma lo mismo personal fijo o temporal, propio, desplazado o subcontratado. Cuando se subcontraten servicios, se imputará la carga de trabajo indicada en el contrato de prestación de servicios.

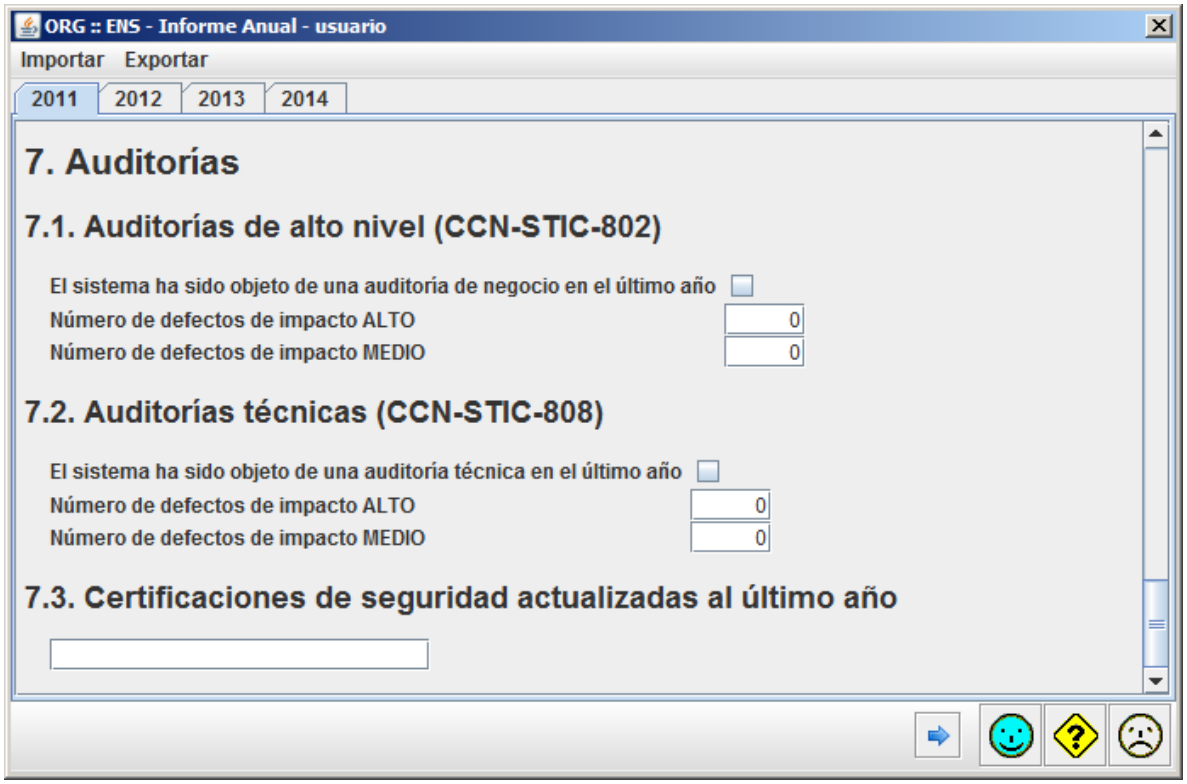
53. Porcentajes objetivo dedicados a los diferentes conceptos de seguridad TIC:

	categoría		
indicador	BAJA	MEDIA	ALTA
STIC/TIC	3%	5%	10%
concienciación y formación			
personal externo			
servicios externos			
productos			

54. Umbrales: porcentajes dedicados a seguridad TIC. Relativos al valor objetivo central.

- 50% - rojo inferior
- 66% - amarillo inferior
- 150% - amarillo superior
- 200% - rojo superior

2.8 AUDITORÍAS



2.8.1 AUDITORÍAS DE ALTO NIVEL

55. Guía CCN-STIC 802

etiqueta	audit.biz.b
descripción	El sistema ha sido objeto de una auditoría de alto nivel en el último año
tipo	boolean
valores	true | false

etiqueta	audit.biz.high
descripción	Número de defectos de nivel ALTO encontrados en la última auditoría
tipo	entero
valores	≥ 0

etiqueta	audit.biz.medium
descripción	Número de defectos de nivel MEDIO encontrados en la última auditoría
tipo	entero
valores	≥ 0

2.8.2 AUDITORÍAS TÉCNICAS

57. Guía CCN-STIC 808

etiqueta	audit.tech.b
descripción	El sistema ha sido objeto de una auditoría técnica de alto nivel en el último año
tipo	boolean
valores	true | false

etiqueta	audit.tech.high
descripción	Número de defectos de nivel ALTO encontrados en la última auditoría técnica
tipo	entero
valores	≥ 0

etiqueta	audit.tech.medium
descripción	Número de defectos de nivel MEDIO encontrados en la última auditoría técnica
tipo	entero
valores	≥ 0

2.8.3 CERTIFICACIONES DE SEGURIDAD ACTUALIZADAS AL ÚLTIMO AÑO

etiqueta	s_certs
descripción	Certificaciones de seguridad actualizadas al último año.
tipo	texto
valores	formato libre

2.9 KRI – KEY RISK INDICATORS

2.9.1 DERECHOS DE LOS USUARIOS

58. Se refiere a los equipos cliente empleados por el personal o trabajadores del organismo.

etiqueta	client.conf_p
descripción	Porcentaje de 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
tipo	porcentaje
valores	0% .. 100%
objetivo	100%

2.9.2 DISPOSITIVOS PROPIOS DEL USUARIO (BYOD)

59. Se refiere a personal o trabajadores del organismo que emplean dispositivos propios para acceder a los sistemas. Por ejemplo, portátiles, tabletas, smart phones, etc.

etiqueta	byod_p
descripción	Porcentaje de equipos de los usuarios internos (BYOD) sobre el total de equipos del sistema
tipo	porcentaje
valores	0% .. 100%

etiqueta	byod.conf_p
descripción	Porcentaje de equipos de los usuarios internos (BYOD) sobre el total de equipos del sistema en los que la configuración y su gestión están bajo control exclusivo de los técnicos del organismo
tipo	porcentaje
valores	0% .. 100%
objetivo	100%

2.9.3 ROTACIÓN DE PERSONAL

60. Indicador predictivo.

etiqueta	people.churn
descripción	tasa de rotación de personal
tipo	porcentaje
fórmula	stic_p = número de personas dedicadas a seguridad TIC (media del año) people.out = número de personas dedicadas a seguridad TIC que abandonan el organismo en el último año people.churn = people.out / stic_p
valores	0% .. 100%
objetivo	< 10%

3. SISTEMA(S) DE INFORMACIÓN

61. En esta sección se trata de caracterizar el o los sistemas de información evaluados. Tiene interés a efectos estadísticos, aunque también proporciona una foto de alto nivel de lo que maneja el organismo.

3.1 ACTIVOS ESENCIALES

62. Por cada activo esencial, su valoración en cada dimensión de seguridad.

activo	tipo	D	I	C	A	T
	☐ información ☐ servicio					
	☐ información ☐ servicio					
	☐ información ☐ servicio					
	☐ información ☐ servicio					

3.2 CUMPLIMIENTO DEL ANEXO II DEL ENS

medidas		madurez o n.a.
org	**Marco organizativo**	
[org.1]	Política de seguridad	
[org.2]	Normativa de seguridad	
[org.3]	Procedimientos de seguridad	
[org.4]	Proceso de autorización	

op	**Marco operacional**	
[op.pl]	Planificación	
[op.pl.1]	Análisis de riesgos	
[op.pl.2]	Arquitectura de seguridad	
[op.pl.3]	Adquisición de nuevos componentes	
[op.pl.4]	Dimensionamiento / Gestión de capacidades	
[op.pl.5]	Componentes certificados	
[op.acc]	Control de acceso	
[op.acc.1]	Identificación	
[op.acc.2]	Requisitos de acceso	
[op.acc.3]	Segregación de funciones y tareas	
[op.acc.4]	Proceso de gestión de derechos de acceso	
[op.acc.5]	Mecanismo de autenticación	
[op.acc.6]	Acceso local (local logon)	
[op.acc.7]	Acceso remoto (remote login)	
[op.exp]	Explotación	
[op.exp.1]	Inventario de activos	
[op.exp.2]	Configuración de seguridad	
[op.exp.3]	Gestión de la configuración	
[op.exp.4]	Mantenimiento	
[op.exp.5]	Gestión de cambios	
[op.exp.6]	Protección frente a código dañino	
[op.exp.7]	Gestión de incidentes	
[op.exp.8]	Registro de la actividad de los usuarios	
[op.exp.9]	Registro de la gestión de incidentes	
[op.exp.10]	Protección de los registros de actividad	
[op.exp.11]	Protección de claves criptográficas	
[op.ext]	Servicios externos	
[op.ext.1]	Contratación y acuerdos de nivel de servicio	
[op.ext.2]	Gestión diaria	
[op.ext.9]	Medios alternativos	
[op.cont]	Continuidad del servicio	

[op.cont.1]	Análisis de impacto	
[op.cont.2]	Plan de continuidad	
[op.cont.3]	Pruebas periódicas	
[op.mon]	Monitorización del sistema	
[op.mon.1]	Detección de intrusión	
[op.mon.2]	Sistema de métricas	

mp	**Medidas de protección**	
[mp.if]	Protección de las instalaciones e infraestructuras	
[mp.if.1]	Áreas separadas y con control de acceso	
[mp.if.2]	Identificación de las personas	
[mp.if.3]	Acondicionamiento de los locales	
[mp.if.4]	Energía eléctrica	
[mp.if.5]	Protección frente a incendios	
[mp.if.6]	Protección frente a inundaciones	
[mp.if.7]	Registro de entrada y salida de equipamiento	
[mp.if.9]	Instalaciones alternativas	
[mp.per]	Gestión del personal	
[mp.per.1]	Caracterización del puesto de trabajo	
[mp.per.2]	Deberes y obligaciones	
[mp.per.3]	Concienciación	
[mp.per.4]	Formación	
[mp.per.9]	Personal alternativo	
[mp.eq]	Protección de los equipos	
[mp.eq.1]	Puesto de trabajo despejado	
[mp.eq.2]	Bloqueo de puesto de trabajo	
[mp.eq.3]	Protección de equipos portátiles	
[mp.eq.9]	Medios alternativos	
[mp.com]	Protección de las comunicaciones	
[mp.com.1]	Perímetro seguro	
[mp.com.2]	Protección de la confidencialidad	
[mp.com.3]	Protección de la autenticidad y de la integridad	
[mp.com.4]	Segregación de redes	
[mp.com.9]	Medios alternativos	
[mp.si]	Protección de los soportes de información	
[mp.si.1]	Etiquetado	
[mp.si.2]	Criptografía	
[mp.si.3]	Custodia	
[mp.si.4]	Transporte	
[mp.si.5]	Borrado y destrucción	

[mp.sw]	Protección de las aplicaciones informáticas	
[mp.sw.1]	Desarrollo	
[mp.sw.2]	Aceptación y puesta en servicio	
[mp.info]	Protección de la información	
[mp.info.1]	Datos de carácter personal	
[mp.info.2]	Calificación de la información	
[mp.info.3]	Cifrado	
[mp.info.4]	Firma electrónica	
[mp.info.5]	Sellos de tiempo	
[mp.info.6]	Limpieza de documentos	
[mp.info.9]	Copias de seguridad *(backup)*	
[mp.s]	Protección de los servicios	
[mp.s.1]	Protección del correo electrónico	
[mp.s.2]	Protección de servicios y aplicaciones web	
[mp.s.8]	Protección frente a la denegación de servicio	
[mp.s.9]	Medios alternativos	

64. Niveles

- n.a. – no es de aplicación en este sistema
- L0 – inexistente
- L1 – ad-hoc – iniciado, pero incipiente
- L2 – reproducible pero intuitivo – se hace de forma artesanal
- L3 – existe y se sigue un procedimiento escrito
- L4 – se mide el desempeño de la función
- L5 – se sigue un proceso de mejora continua

65. Umbrales de madurez;

categoría	rojo inferior	amarillo inferior
ALTA	L3	L4
MEDIA	L2	L3
BAJA	L1	L2

4. XML

66. Para reportar los datos de un organismo se empleará un formato XML como el que se describe a continuación, que facilitará la elaboración estadística de un panorama global compuesto por varios organismos, e incluso de 1 organismo que gestiona varios sistemas de información analizados por separado.

67. El fichero XML tendrá el siguiente formato:

```
<?xml version="1.0" encoding="UTF-8" ?>
<metrics id=”ens” >
  { activo_esencial }*
  { reporte_anual }*
</metrics>

activo_esencial ::=
  <asset code type >
    <name> texto </name>
    { valoración }*
  </asset>

valoración ::=
  <value dimension level />

reporte_anual ::=
  <report version=”2” phase >
    { medida_de_protección }*
    otros
  </report>

medida_de_protección ::=
  <perfil item >
    madurez
  </perfil>
```

68. La versión del REPORT es la 2 para referirse a esta versión de la guía 824.

69. Actualmente se trabaja con los perfiles

```
ens – Esquema Nacional de Seguridad, Anexo II
ip – Guía CCN-STIC-811 Interconexión
```

pero está previsto que se puedan incorporar otros perfiles en el futuro.

atributo	ejemplo	descripción
code	code=”info”	código del activo
type	type=”i”	tipo de activo: i información s servicio is información + servicio
dimension	dimension=”C”	dimensión de seguridad: D disponibilidad I integridad C confidencialidad A autenticidad T trazabilidad
level	level=”A”	valoración (anexo i del ENS) A nivel ALTO M nivel MEDIO B nivel BAJO
item	item=”org.4”	acrónimo de la medida en el anexo ii del ENS

70. La madurez puede ser

n.a.	cuando no aplica
min-max	siendo min y max valores de madurez:
_	valor en blanco
L0	nivel L0 – no existe
L1	nivel L1 – ad-hoc
L2	nivel L2 – informal
L3	nivel L3 – se sigue un procedimiento escrito
L4	nivel L4 – se mide
L5	nivel L5 – mejora continua

4.1 EJEMPLO DE ACTIVOS

```
<asset type="i" code="info">
  <name>información</name>
  <value dimension="I" level="A"/>
  <value dimension="C" level="A"/>
  <value dimension="A" level="A-"/>
  <value dimension="T" level="A"/>
</asset>
<asset type="s" code="servicio">
  <name>servicio prestado</name>
  <value dimension="D" level="B"/>
</asset>
```

4.2 EJEMPLO DE MEDIDAS DE PROTECCIÓN

```
<ens item=”op.exp.3”>_-L4</ens>

<ip item=”A.tools.ids”>L0</ip>
```

4.3 ETIQUETAS DEFINIDAS PARA OTROS

71. Nótese que el informe puede añadir otras etiquetas aprovechando la flexibilidad del formato XML. Esta característica se empleará para extender el conjunto en el futuro sin hipotecar los datos recopilados en el pasado.

72. El formato será el siguiente

    - etiqueta según las tablas donde se definen los indicadores
    - valor según el tipo del indicador
        - números reales: notación internacional (punto decimal)
        - porcentajes: número real entre 0.0 y 1.0
        - booleanos: true o false

73. Ejemplos

    - <audit.biz.high>0</audit.biz.high>
    - <incidents.s.t50_high>5.2</incidents.s.t50_high>
    - <aw.nhp>0.40</aw.nhp>
    - <budget.stic_p>0.05</budget.stic_p>
    - <audit.biz.b>false</audit.biz.b>

5. REFERENCIAS

CCN-STIC-815

Indicadores y Métricas en el ENS
23.4.2012

ENS

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE de 29 de enero de 2010. https://www.ccn-cert.cni.es/publico/ens/ens/index.html