

IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

Acciones de la DTIC. Actualización del ENS y Nivel de cumplimiento

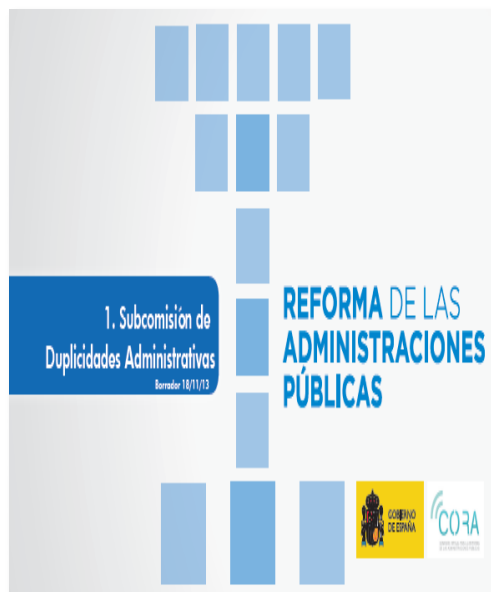


- Miguel A. Amutio Gómez
- MINHAP - DTIC
- miguel.amutio@seap.minhap.es

Acciones de la DTIC

Actualización del ENS

Cumplimiento con el ENS



✓ Creación de la figura del DTIC de la AGE

-> RD 802/2014

✓ Nuevo modelo de gobernanza TIC

-> RD 806/2014

✓ Consolidación y servicios comunes

-> RD 802/2014,
RD 806/2014

Acciones de la DTIC



PLAN DE TRANSFORMACIÓN
DIGITAL DE LA ADMINISTRACIÓN
GENERAL DEL ESTADO Y SUS
ORGANISMOS PÚBLICOS

(ESTRATEGIA TIC)
2015 - 2020

Estrategia TIC



GOBIERNO
DE ESPAÑA

MINISTERIO
DE HACIENDA
Y ADMINISTRACIONES PÚBLICAS

SECRETARÍA DE ESTADO DE
ADMINISTRACIONES PÚBLICAS

DIRECCIÓN DE TECNOLOGÍAS DE LA
INFORMACIÓN Y LAS COMUNICACIONES

Objetivo V: Estrategia corporativa de seguridad y usabilidad

Línea de acción 9

Garantizar la seguridad de los sistemas de información de la AGE y sus organismos públicos

El Esquema Nacional de Seguridad introduce los elementos necesarios para generar confianza en el uso de los medios electrónicos para que los ciudadanos puedan relacionarse con la Administración digitalmente con plena garantía y seguridad.

Para ello, dispone un conjunto de medidas a aplicar en las redes y sistemas de información de los que es titular la Administración. El ENS se enfoca fundamentalmente en todos aquellos sistemas que dan soporte a un servicio público dirigido al ciudadano o empresa. Es necesario ampliar ese enfoque, e iniciar ciclos de mejora continua en la protección de todos los sistemas de información.

Además, es necesario tener en cuenta el equilibrio entre seguridad y usabilidad, así como avanzar en aumentar la disponibilidad de los sistemas y publicarlos.

Esta línea está directamente relacionada con el objetivo 1 de la Estrategia Nacional de Ciberseguridad, como contribución a la misma.

- Ampliación del alcance del ENS a todos los Sistemas de Información de las AA.PP. españolas, al objeto de ampliar los beneficios derivados de su implantación y facilitar su plena implantación según lo previsto en la Estrategia de Ciberseguridad Nacional.
- Informar sobre la disponibilidad de los servicios y para aquellos servicios más críticos indicar el porcentaje máximo de indisponibilidad.
- Crear un entorno que confiera al ciudadano seguridad al hacer uso de los servicios públicos digitales.
- Desarrollar una Política de Seguridad Común a toda la AGE y sus organismos públicos.
- Implantar una plataforma común de seguridad gestionada que permita garantizar unos niveles mínimos y aceptables de seguridad para todos los organismos.

Declaración de Servicios compartidos

1. Servicio unificado de telecomunicaciones

2. Servicio de seguridad gestionada

3. Servicio de alojamiento de infraestructuras TIC
4. Servicio de nube híbrida (Nube SARA)
5. Servicio de correo electrónico unificado
6. Servicio multicanal de atención al ciudadano
7. Servicio de gestión del registro
8. Servicio de gestión de notificaciones
9. Servicio de gestión de nómina
10. Servicio integrado de gestión de personal
11. Servicio común de gestión económico-presupuestaria
12. Servicio común de generación y validación de firma-e
13. Servicio de gestión de expediente y documento-e
14. Servicio de gestión de archivo electrónico



2.2. SERVICIO DE SEGURIDAD GESTIONADA

Descripción:

Conjunto de servicios de ciberseguridad que proporcionan protección a la AGE y sus Organismos Públicos; incluye el equipamiento necesario, así como su configuración, puesta en marcha, mantenimiento y gestión.

Persigue una infraestructura global y única complementaria al servicio compartido de Telecomunicaciones, así como de una serie de servicios gestionados por personal especializado:

- seguridad perimetral,
- navegación segura,
- correo seguro,
- acceso remoto,
- anti-amenazas persistentes avanzadas,
- prevención de fugas de información,
- cortafuegos de aplicaciones,
- anti suplantación,
- auditorías de vulnerabilidades,
- autenticación Kerberos contra directorio activo de los centros adheridos,
- examen de tráfico SSL integrado con el HSM y PKI de los centros adheridos,
- otros servicios auxiliares de carácter horizontal, como balanceo geográfico entre CPDs, presentación IPV6, visibilidad, priorización y categorización del tráfico y gestión de los eventos y de la información de seguridad.

En general, los servicios se proporcionarán desde una perspectiva multi-cliente. Cada entidad podrá prescribir sus propias políticas de seguridad, que serán implementadas y gestionadas por personal especializado del Centro de Operaciones de Seguridad de la AGE y sus OOPP (COS). Asimismo, se pueden ofrecer servicios adaptados a las necesidades específicas de las distintas entidades que se adhieran al servicio.

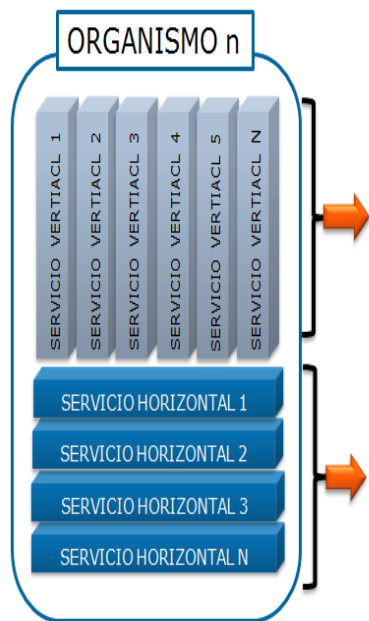
Servicio de seguridad gestionada

✓ **Conjunto de servicios** de seguridad de la red perimetral **para protección del acceso a Internet** de la AGE y sus Organismos Públicos.

- Incluye todo el equipamiento necesario, así como su configuración, puesta en marcha, mantenimiento y gestión.
- Infraestructura global y única **complementaria a los servicios y equipamientos del servicio de telecomunicaciones** de la AGE en su faceta de acceso a Internet, así como de una serie de servicios asociados a la misma.

✓ Servicios proporcionados desde **perspectiva multi-cliente**.

- ✓ **Cada organismo podrá establecer sus propias políticas de seguridad**, que serán implementadas y gestionadas de forma autónoma por personal especializado.
- ✓ **Se pueden ofrecer servicios adaptados** a las necesidades específicas de las distintas Entidades que se adhieran al servicio.



SERVICIOS HORIZONTALES (básicos):

- ✓ Servicio de *ticketing* de incidentes (Herramienta LUCIA)
- ✓ Servicio de análisis (Herramienta CARMEN)
- ✓ Servicio básico de cortafuegos de siguiente generación e IPS
- ✓ SIEM y servicio de logs
- ✓ Servicio de auditoría de vulnerabilidades
- ✓ Servicio anti amenazas persistentes avanzadas
- ✓ Servicio de cortafuegos de aplicaciones web
- ✓ Aplicación de arquitecturas de referencia
- ✓ Infraestructura básica de producción y gestión
- ✓ DNS, presentación IPv6, balanceo de carga

SERVICIOS VERTICALES (Opcionales / Se solicitan por cada Organismo o Entidad):

- ✓ Servicio de acceso remoto VPN (red privada virtual)
- ✓ Dispositivos móviles (VPN, comunicaciones seguras)
- ✓ Servicio de cortafuegos de siguiente generación e IPS
- ✓ Servicio de navegación segura (filtrado de URLs, *antivirus*, *anti malware*, *anti-botnets*, *proxy*)
- ✓ Servicio de correo seguro (*antivirus*, *anti-spam*)
- ✓ Servicio de prevención anti fuga de información (DLP)
- ✓ Servicio contra la suplantación de la identidad digital

Más información: <https://www.ccn-cert.cni.es/>

Centro de operaciones de seguridad

✓ **Aglutina las funciones** de gestión, operación, mantenimiento, provisión, administración, tratamiento de incidentes de seguridad y generación de informes, garantizando los niveles de servicio y calidad.

✓ **Funciones basadas en políticas de seguridad** del Sector Público Estatal y en lo dispuesto en el Esquema Nacional de Seguridad.

✓ **En cada Organismo o Entidad existirá un responsable TIC** que será el encargado de designar los permisos y **puntos de contacto** con el COS.

✓ Niveles de prestación de servicio con roles y responsabilidades:

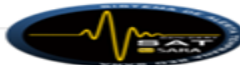
- **Dirección y Supervisión:** supervisión y establecimiento de las normas y políticas de aplicación general, así como la gestión en otras instancias cuando se presuma responsabilidad legal.
- **COS Nivel 1.** Operación e Implementación: implantación, mantenimiento y continuidad del servicio.
- **COS Nivel 2.** Inteligencia de seguridad: directrices técnicas, asistencia al escalado del Nivel 1 y aportación de inteligencia a las operaciones de seguridad.
- **COS Nivel 3.** CCN



Herramientas y servicios de



- ✓ Uso de **herramientas de prevención, detección y corrección** proporcionadas por CCN y CCN-CERT (herramientas y COS nivel 3).
- ✓ **Interacción con CCN-CERT.**
- ✓ **Herramientas de prevención y corrección** disponibles en el catálogo de productos certificados (<https://oc.ccn.cni.es/>).

- ✓  : Sistema Alerta Temprana **INTERNET**
- ✓  **CARMEN**: Centro de Análisis de Registros y Minería de Eventos
- ✓ **LUCIA** : Listado Unificado de Coordinación de Incidentes y Amenazas
- ✓  : Informe Nacional del Estado de Seguridad.
- ...



Actualización del ENS



BOE BOLETÍN OFICIAL DEL ESTADO 

Núm. 25 Viernes 29 de enero de 2010 Sec. I. Pág. 8089

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA

1330 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 BOLETÍN OFICIAL DEL ESTADO 

Núm. 254 Miércoles 4 de noviembre de 2015 Sec. I. Pág. 104246

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA

11881 Real Decreto 951/2015, de 23 de octubre, de modificación del 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.



***Real Decreto 951/2015**

Aspectos principales de la actualización (I/IV)

- ✓ Se enfatiza **la gestión continuada de la seguridad** (art.11):

*Todos los órganos superiores de las Administraciones públicas **deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad**, que será aprobada por el titular del órgano superior correspondiente.*

- ✓ Se introduce la noción de **profesionales cualificados** (art.15).
- ✓ **En la adquisición de productos certificados** se introduce la **noción de la proporcionalidad** vinculada a la categoría del sistema y nivel de seguridad determinados y a los riesgos (art. 18).
- ✓ Se refuerza la **gestión de incidentes** (art. 24)

Aspectos principales de la actualización (II/IV)

- ✓ La relación de medidas seleccionadas del anexo II se formalizará en un documento denominado **Declaración de Aplicabilidad**, firmado por el responsable de seguridad (art. 27).
- ✓ Las medidas de seguridad referenciadas en el anexo II podrán ser reemplazadas por otras **compensatorias** siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (art. 27).
- ✓ Se introducen la figura de las **instrucciones técnicas de seguridad** para señalar el modo común de actuar (art. 29) en ciertas cuestiones.

Aspectos principales de la actualización (III/IV)

- ✓ Se mejoran los mecanismos para obtener un **conocimiento regular del estado de la seguridad** en las AA.PP. (art. 35).
- ✓ Se introduce la **notificación de incidentes de seguridad** (art. 36).
- ✓ Se precisan los **elementos necesarios para la investigación de incidentes de seguridad** (art. 37).
- ✓ Se mejora el anexo III de **auditoría de la seguridad**.
- ✓ Se revisa la **clausula de adquisición de productos** de seguridad (anexo V).
- ✓ Adecuación: 24 meses desde el 5 de noviembre.

Aspectos principales de la actualización (IV/IV)

✓ **Se mejoran ciertas medidas** de seguridad (anexo II). Principalmente:

- 3.4 Proceso de autorización [org.4]
- 4.1.2. Arquitectura de seguridad [op.pl.2]
- 4.1.5 Componentes certificados [op.pl.5] + medidas relacionadas
- 4.2.1. Identificación [op.acc.1]
- 4.2.5. Mecanismo de autenticación [op.acc.5]
- 4.3.7. Gestión de incidentes [op.exp.7]
- 4.3.8. Registro de la actividad de los usuarios [op.exp.8]
- 4.3.9. Registro de la gestión de incidentes [op.exp.9]
- 4.6.1. Detección de intrusión [op.mon.1]
- 4.6.2. Sistema de métricas [op.mon.2]
- 5.4.3. Protección de la autenticidad y de la integridad [mp.com.3]
- 5.5.5. Borrado y destrucción [mp.si.5]
- 5.6.1. Desarrollo de aplicaciones [mp.sw.1]
- 5.7.4. Firma electrónica [mp.info.4]
- 5.7.7. Copias de seguridad [mp.info.9]

Apartados: 3.4, 4.1.2, 4.1.5, 4.2.1, 4.2.5, 4.3.3, 4.3.7, 4.3.8, 4.3.9, 4.3.11, 4.4.2, 4.6.1, 4.6.2, 5.2.3, 5.3.3, 5.4.2, 5.4.3, 5.5.2, 5.5.5, 5.6.1, 5.7.4, 5.7.5, 5.7.7 y 5.8.2

Cumplimiento con el ENS



Las **Administraciones Públicas**, y el cumplimiento con el ENS

¿cómo lo manifiestan?

¿lo recogen en sus pliegos?



**Las soluciones que ofrecen los
proveedores a la Administración,
¿son conformes con el ENS?
¿cómo lo manifiestan?**



Conformidad con el ENS



Art. 41: ... darán publicidad en las correspondientes sedes electrónicas a las **declaraciones de conformidad**, y a los **distintivos de seguridad** de los que sean acreedores, obtenidos respecto al cumplimiento del ENS.

Demanda

- ✓ **Órganos y Entidades** de Derecho Público.
- ✓ **Proveedores** de soluciones y tecnología.
- ✓ Prestadores de **servicios de auditoría y certificación**.

Capacidades

- Hay quien sabe:**
- ✓ Auditar y certificar.
 - ✓ Acreditar la competencia técnica.

Pautas

- ✓ Verificación cumplimiento y **publicación de conformidad**.
- ✓ También de soluciones y tecnología.
- ✓ **Auditoría y certificación**.

ÍNDICE

1.	INTRODUCCIÓN.....	4
2.	LA CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD.....	5
2.1.	CRITERIOS DE DETERMINACIÓN DE LA CONFORMIDAD	5
2.2.	PROCEDIMIENTOS DE DETERMINACIÓN DE LA CONFORMIDAD	5
3.	PUBLICIDAD DE LA CONFORMIDAD	8
3.1.	ESQUEMA DE DECLARACIÓN Y CERTIFICACIÓN DE LA CONFORMIDAD CON EL ENS	8
3.2.	DECLARACIÓN DE CONFORMIDAD	8
3.3.	CERTIFICACIÓN DE CONFORMIDAD	8
3.4.	SOLUCIONES Y SERVICIOS PRESTADOS POR EL SECTOR PRIVADO	9
	ANEXO A – MODELOS DE DECLARACIÓN Y SELLO DE CONFORMIDAD CON EL ENS	10
	ANEXO B – MODELOS DE CERTIFICACIÓN Y SELLO DE CONFORMIDAD CON EL ENS.....	12

3.1. ESQUEMA DE DECLARACIÓN Y CERTIFICACIÓN DE LA CONFORMIDAD CON EL ENS

17. La exhibición de una **Declaración de Conformidad** –de aplicación a sistemas de información de categoría BÁSICA- o una **Certificación de Conformidad** –de aplicación a sistemas de información de categorías MEDIA o ALTA- son necesarias para mostrar, a todos los interesados, el compromiso de la entidad en cuestión con la seguridad de los sistemas, respecto de la información que trata o los servicios que presta.
18. Cuando se trate de sistemas de información de categoría MEDIA o ALTA, **el Centro Criptológico Nacional (CCN) y la Entidad Nacional de Acreditación (ENAC), atendiendo a un procedimiento regulado, participarán en la acreditación de las Entidades de Certificación del ENS**, a las que informarán sobre los criterios que deben adoptar para una adecuada evaluación de la conformidad respecto de las auditorías que desarrollen, por sí mismas o por terceros designados, autorizados o seleccionados por ellas, haciendo uso, cuando proceda, de las normas y recomendaciones internacionales específicas a tales propósitos².

² Tales como UNE-EN ISO/IEC 17065:2012, Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios; UNE-EN ISO/IEC 17021:2011 Evaluación de la conformidad. Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión, ó ISO/IEC 27006:2011 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems.

ANEXO A - MODELOS DE DECLARACIÓN Y SELLO DE CONFORMIDAD CON EL ENS

DECLARACIÓN DE CONFORMIDAD CON EL RD 3/2010, DE 8 DE ENERO, POR EL QUE SE REGULA EL ESQUEMA NACIONAL DE SEGURIDAD EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA (ENS)		
Logotipo de la Entidad Pública declarante	Identificación inequívoca del declarante, incluyendo la denominación legal que aprueba la estructura orgánica a la que está adscrito.	
Los sistemas de información reseñados seguidamente, todos ellos de categoría BÁSICA, y conforme a lo dispuesto en el Anexo III del RD 3/2010, han superado un proceso de autoevaluación realizado en las fechas que se indican:		
1.	aaaa/mm/dd	Denominación Sistema de Información 1 y servicios prestados
2.	aaaa/mm/dd	Denominación Sistema de Información 2 y servicios prestados
...	...	...
Dicho proceso de autoevaluación garantiza que los sistemas referenciados cumplen las medidas de seguridad impuestas por el RD 3/2010 para sistemas de categoría BÁSICA.		
En Localidad, a ____ de ____ de 2015		
Fdo. Nombre y Apellidos del Titular del Órgano Superior de que se trate Administración Pública de que se trate		
Evidencias de Firma electrónica [personal / para actuación administrativa automatizada] del declarante		

Nota: Los textos señalados en letra cursiva deben ser adaptados a cada caso.

DECLARACIÓN DE CONFORMIDAD CON EL



Categoría BÁSICA
aaaa / mm / dd

[LOGOTIPO DE LA ENTIDAD CERTIFICADORA]

CERTIFICACIÓN DE CONFORMIDAD CON EL



Categoría [MEDIA/ALTA]
aaaa / mm / dd
Número del certificado: _____

ANEXO B - MODELOS DE CERTIFICACIÓN Y SELLO DE CONFORMIDAD CON EL ENS

RD 3/2010 ENS

Logotipo de la Entidad Certificadora

Certificación
Concedida a Entidad⁽¹⁾
Población Dirección postal

Entidad Certificadora certifica que el Sistema de Información Denominación del Sistema de Información, de categoría ____⁽²⁾, ha sido auditado y encontrado conforme con las exigencias del 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.

Los servicios prestados por el antedicho Sistema de Información son: _____

Declaración de aplicabilidad: versión ____ fecha ____ de ____ de 201__

Fecha de certificación inicial: ____ de ____ de 201__
Fecha de expiración: ____ de ____ de 201__ (3).

Para cualquier aclaración sobre el alcance del presente certificado y la aplicación de los requisitos del ENS, pueden ponerse en contacto con la Entidad Certificadora.

Número del Certificado: _____
Fecha: ____ de ____ de 201__
Firma del responsable de la Entidad Certificadora: _____

Nombre completo / razón social de la Entidad Certificadora y pag. web.
Dirección postal / electrónica.
Oficina de emisión (en su caso).
Código Postal, Provincia, País.

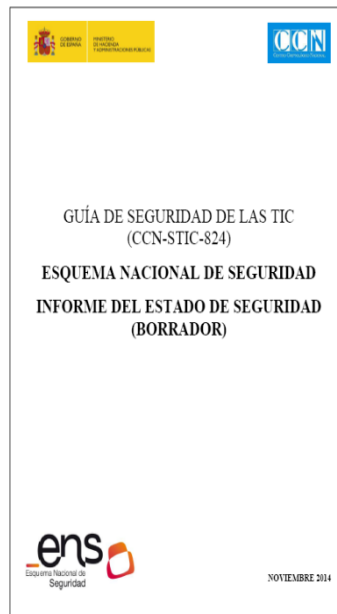
(1) Podiendo ser de naturaleza jurídica pública o privada.
(2) BÁSICA/MEDIA/ALTA.
(3) Máximo de 2 años.

Conocer el estado de la seguridad

El ENS exige:

- ✓ **Informar del estado de la seguridad.**
- ✓ **Medir la seguridad:** 4.6.2 Sistema de métricas [op.mon.2]

SIN CLASIFICAR



La herramienta **'INES'** facilita la recogida y consolidación de información para el *Informe del Estado de la Seguridad* (RD 3/2010, art. 35 y línea de acción 2 de Estrategia de Ciberseguridad Nacional).



Registro portal CCN-CERT
Acceso a INES:
ines@ccn-cert.cni.es

18.12.2015 Fin plazo recogida de datos

Situación Fuente: INES

	AGE	CCAA	LOCAL
Proceso de autorización	60	50	60
Análisis de riesgos	50	50	50
AGE	CCAA	EELL	
92.0	60.0	99.5	
Gestión de la configuración	26	25	30
Gestión de cambios	30	28	25
Continuidad de operaciones	5	5	2



Herramienta de auditoría de cumplimiento con el
ENS/STIC en Sistemas Windows.

- Auditoría integral de cumplimiento en sistemas Windows
- Sencilla, intuitiva y lista para utilizar
- Adaptable a múltiples escenarios
- Resultados fiables y de fácil interpretación
- Reducción de costes y tiempo de auditoría

clara@ccn-cert.cni.es

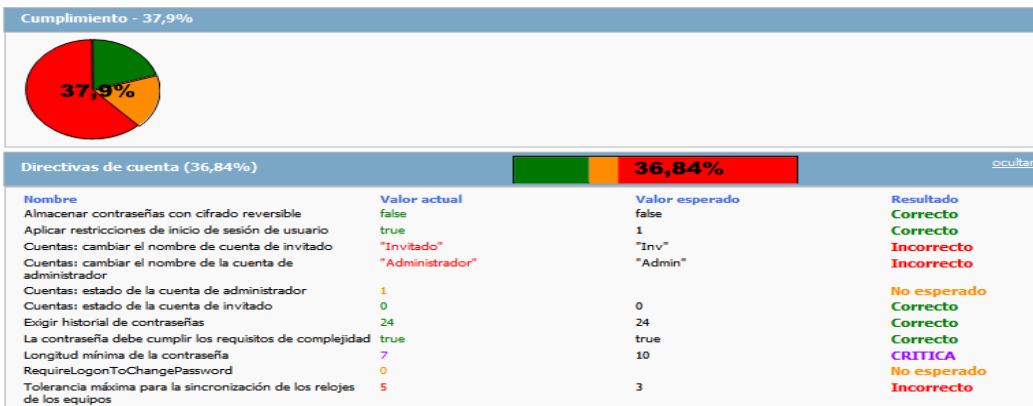
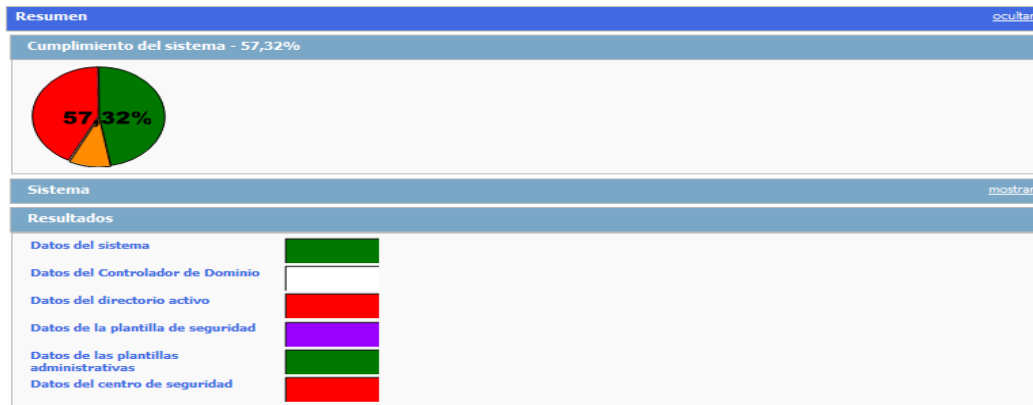
Informes de Auditoría

Información Ejecutiva



Herramienta de auditoría de cumplimiento con el ENS/STIC en Sistemas Windows.

Información Técnica



Esfuerzo colectivo



- ✓ El RD 3/2010, Guías CCN-STIC (Serie 800), seguimiento, herramientas, servicios...

Pero sobre todo:

- ✓ Esfuerzo colectivo de **todas las AA.PP.** (AGE, CC.AA., EE.LL. (FEMP), Universidades (CRUE), ámbito de Justicia (EJIS), **coordinado por MINHAP y CCN.**
- ✓ **+ Industria** sector seguridad TIC.
- ✓ **Convencimiento común:** gestión continuada de la seguridad, con un tratamiento homogéneo y adaptado al quehacer de la Administración.

El medio electrónico como medio habitual



Guías CCN-STIC :

- 800 - Glosario de Términos y Abreviaturas del ENS
- 801 - Responsables y Funciones en el ENS
- 802 - Auditoría de la seguridad en el ENS
- 803 - Valoración de sistemas en el ENS
- 804 - Medidas de implantación del ENS
- 805 - Política de Seguridad de la Información
- 806 - Plan de Adecuación del ENS
- 807 - Criptología de empleo en el ENS
- 808 - Verificación del cumplimiento de las medidas en el ENS
- 809 - Declaración de Conformidad del ENS
- 810 - Creación de un CERT / CSIRT
- 811 - Interconexión en el ENS
- 812 - Seguridad en Entornos y Aplicaciones Web
- 813 - Componentes certificados en el ENS
- 814 - Seguridad en correo electrónico
- 815 - Métricas e Indicadores en el ENS
- 817 - Gestión de Ciberincidentes
- 818 - Herramientas de Seguridad en el ENS
- 820 - Protección contra Denegación de Servicio
- 821 - Ejemplos de Normas de Seguridad
- 822 - Procedimientos de Seguridad en el ENS
- 823 – Cloud Computing en el ENS
- 824 - Informe del Estado de Seguridad
- 825 – ENS & 27001
- 827 - Gestión y uso de dispositivos móviles
- 844 - Manual de usuario de INES
- 850A - Implantación del ENS en Windows 7 (cliente en dominio)
- 850B - Implementación del ENS en Windows 7 (cliente independiente)

- 851A - Implementación del ENS en Windows Server 2008 R (controlador dominio y servidor miembro)
- 851B - Implementación del ENS en Windows Server 2008 R2 (servidor Independiente)
- 859 - Recolección y consolidación de eventos con Windows Server 2008 R2
- 860 - Seguridad en el Servicio Outlook Web App (OWA) de MS Exchange Server 2010
- 869 - Implementación de AppLocker en el ENS
- 870A - Implementación del ENS en Windows Server 2012 R2 (controlador de dominio y servidor miembro)
- 870B - Implementación del ENS en Windows Server 2012 R2 (servidor independiente)
- MAGERIT v3 – Metodología de análisis y gestión de riesgos de los sistemas de información

Herramientas de ciberseguridad:

Pilar, INÉS, CLARA, LUCÍA, CARMEN, ...



Muchas gracias



➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es



Síguenos en Linked in

