Desafíos de la transformación digital en las Administraciones locales: ciberseguridad e inteligencia artificial

Implantación del Esquema Nacional de Seguridad y gobernanza de la ciberseguridad

Juan Trastoy

Responsable de Seguridad de la Información

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

juan.trastoy@us

Segovia, 11 de abril de 2024

Esquema Nacional de Seguridad

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Esque

RD 3/2

Applus

CERTIFICADO

No. ENS-0332/22

CERTIFICADO DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

LGAI TECHNOLOGICAL CENTER, S.A. (Applus+) certifica que los sistemas de información reseñados, todos ellos de categoría *MEDIA*, y los servicios que se relacionan, de

UNIVERSIDAD DE SANTIAGO DE COMPOSTELA (USC)

USC- Rectorado Universidad
Pazo San Xerome – Praza do Obradorio - 15704, Santiago de Compostela (A Coruña)

Área de Tecnologías de la Información y de las Comunicaciones (ATIC)
Pavillón de Servizos – Campus Vida, Rúa de José María Suárez Núñez, s/n - 15782, Santiago de Compostela (A Coruña)

Han sido auditados y encontrados 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, según se indica en el correspondiente informe de Auditoría de 30/06/2022 y 01/07/2022 para:

Los sistemas de información que dan soporte a los servicios de: Gestión Académica, Gestión de Personal, Sede Electrónica, Calidade, Deportes, Docencia Virtual. Según la declaración de aplicabilidad ENS.DOC. SEG.01 de fecha 23/06/2022

Fecha de certificación de conformidad inicial: 09/1
Fecha de renovación de la certificación de confor
Madrid a, 09/12/2022

[redacted]

04/05/2024

Directora Técnica
Applus Certification, B.U.
BACHILLER MARTINEZ CRISTINA - 50311639J
Firmado digitalmente por BACHILLER MARTINEZ CRISTINA - 50311639J
Fecha: 2022.12.12 13:22:17 +01'00'
Cristina Bachiller Martínez

Applus certification

LGAI TECHNOLOGICAL CENTER, S.A (Applus+)
Ronda de la Font del Carme, s/n (Campus UAB)
08193 Bellaterra (Cerdanyola del Vallès) BARCELONA (ESPAÑA)
URL: www.appluscertification.com

ENAC CERTIFICACIÓN ISO 17065 Nº12 / C-PR041

ens

Esquema Nacional de Seguridad

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

CERTIFICACIÓN DE CONFORMIDAD CON EL

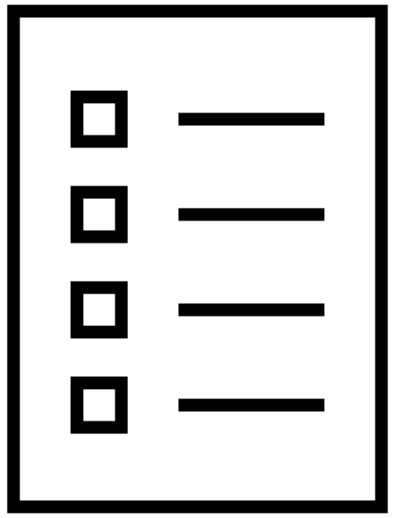
Esquema Nacional de Seguridad

Categoría MEDIA

RD 3/2010 → RD 311/2022

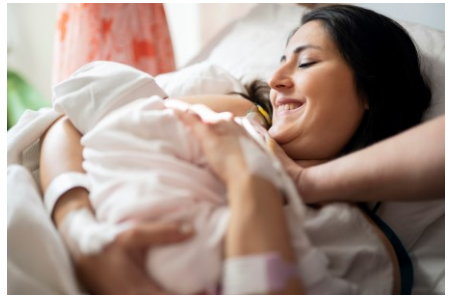
Juan Trastoy

¿Cómo nos enfrentamos al ENS?



El ENS da

- **Miedo**
- **Terror**
- **Está chupado**
- **Ninguna de las anteriores**



Es como tu madre:

Te dice, insistentemente, lo que tienes que hacer y cómo hacerlo. Sabes que tiene razón, pero desearías que te dejara tranquilo.

Cada medida que se tome para mejorar la seguridad provocará reacciones negativas.

Serán impopulares y habrá una fuerte resistencia.

Juan Trastoy

¿Cómo nos enfrentamos al ENS?

Concienciación y formación para

Formación, capacitación y talento en ciberseguridad

ángeles

Centro Criptológico Nacional

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

 # Itinerarios de formación

El Plan de Formación del Centro Criptológico Nacional ofrece un amplio programa de cursos formativos, adaptado a las necesidades planteadas por su comunidad de referencia.

 # Cursos STIC

Acciones formativas en materia de Seguridad de las Tecnologías de la Información y la Comunicación.

Kit de concienciación

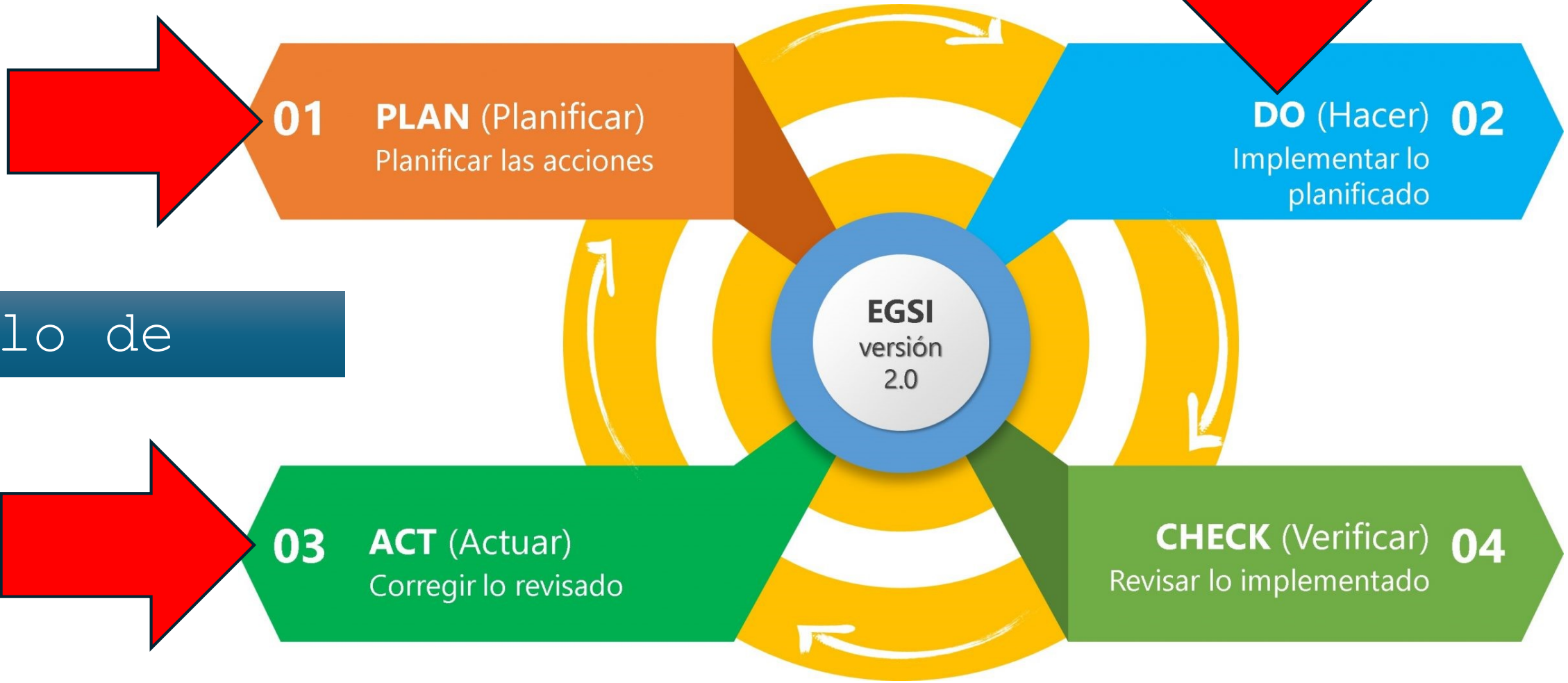
https://www.incibe.es/empresas/formacion/kit-concienciacion

Paciencia, fuerza y decisión para

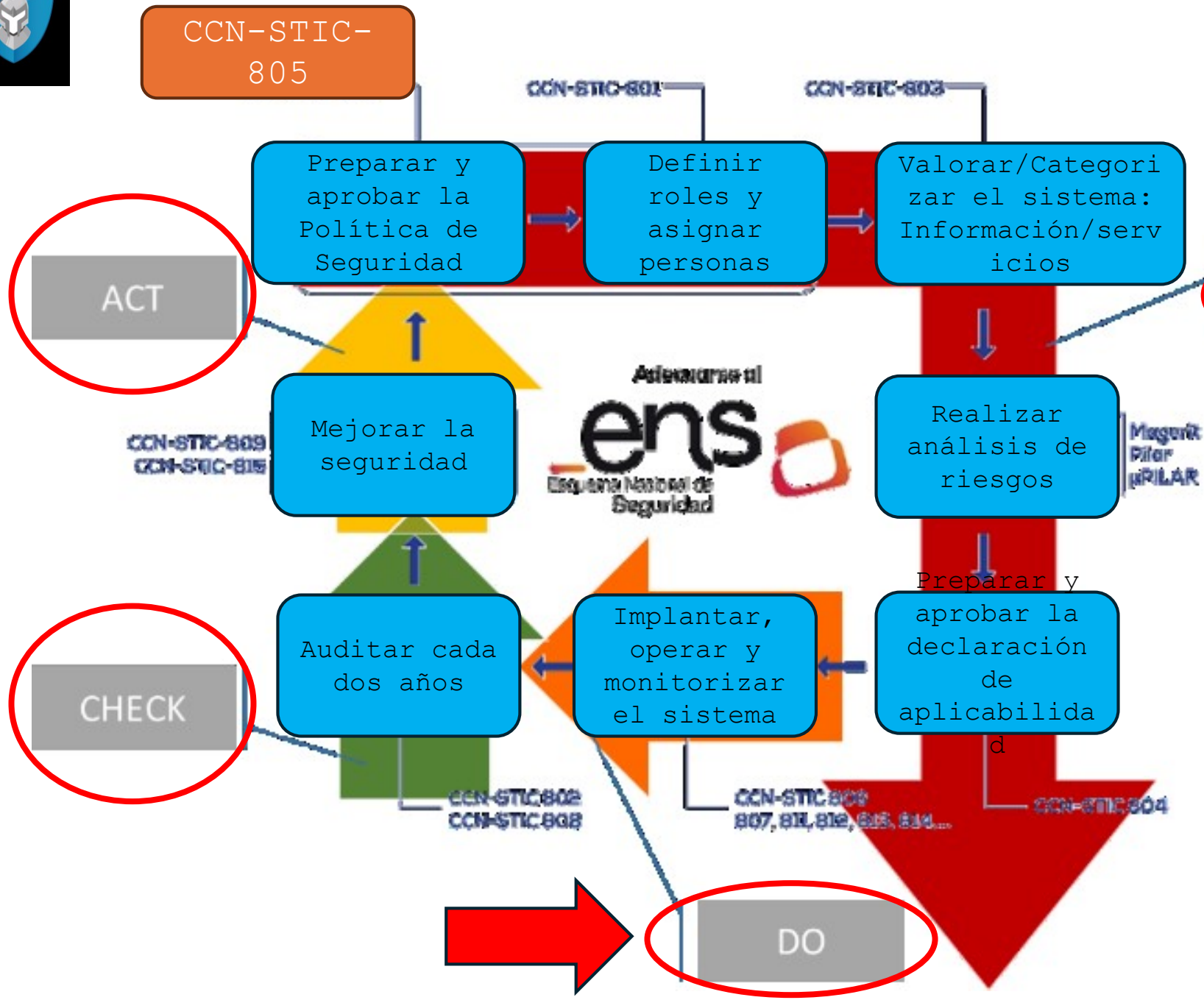
Juan Trastoy

¿Cómo nos enfrentamos al ENS?

Ciclo de



Juan Trastoy



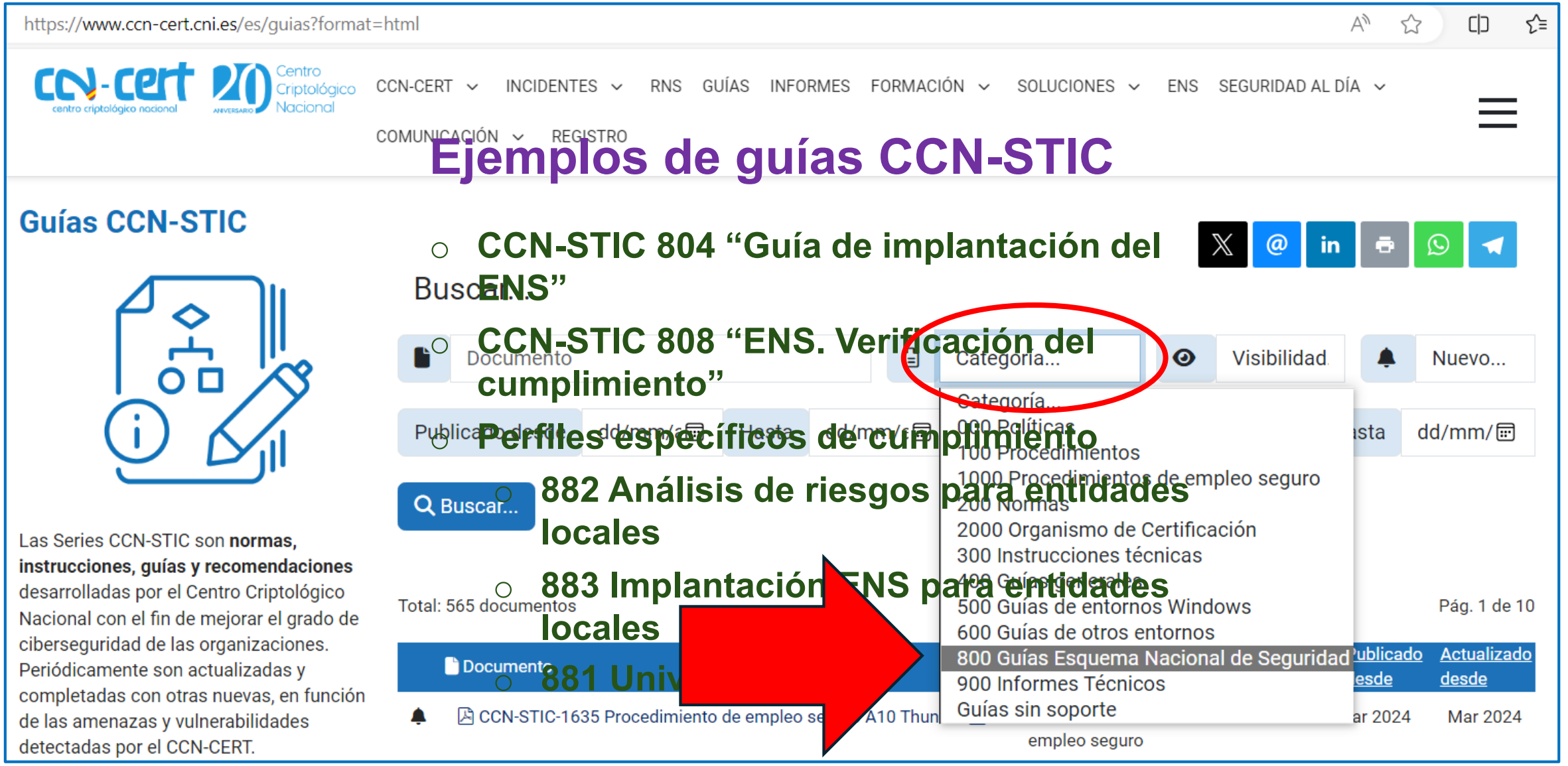
El ENS no impone ninguna metodología concreta para el análisis y gestión de los riesgos más allá de la necesidad de utilizar una metodología reconocida, cuya funcionalidad y resultados puedan ser contrastables.

La metodología MAGERIT está muy evolucionada y extendida en el sector público, habiendo otras metodologías y normas genéricas, como puede ser la ISO 31000:2018 sobre directrices para la gestión del riesgo, que no se contradicen, sino que más bien se complementan.

Juan Trastoy

Ejemplos de guías CCN-STIC

- CCN-STIC 804 “Guía de implantación del ENS”
- CCN-STIC 808 “ENS. Verificación del cumplimiento”
- Perfiles específicos de cumplimiento
  - 882 Análisis de riesgos para entidades locales
  - 883 Implantación ENS para entidades locales
  - 881 Univ



Proyecto de adecuación al ENS

1. Fase PLAN

- **Elaboración y revisión de normativa**

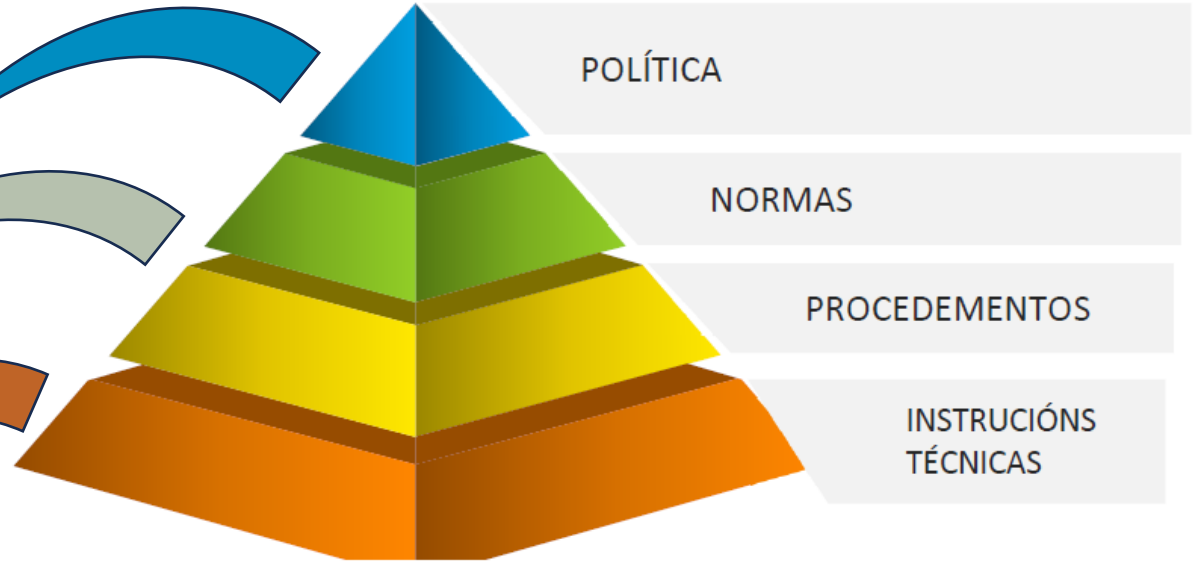
Juan Trastoy

Decir lo que vamos a hacer

Hacer lo que hemos dicho que íbamos a

Evaluar como lo hemos

DOCUMENTACIÓN DEL SISTEMA DE INFORMACIÓN



Política de Seguridad de la Información

Normas específicas y procedimientos que regulan aspectos concretos de la seguridad (por ejemplo, el proceso de autorización para el acceso a la información, la salida de información fuera de la entidad, la organización de la seguridad física y lógica, la contratación y seguimiento de proveedores,...)

Instrucciones técnicas a seguir para realizar acciones concretas (por ejemplo, el modo de dar de alta a un usuario en un sistema de información, hacer copias de seguridad,...)

Proyecto de adecuación al ENS

1. Fase PLAN

- **Elaboración y revisión de normativa**
- **Definir roles y asignar personas**

ROLES Y RESPONSABILIDADES

- Responsable de la información
  - Alta dirección
  - ¡¡¡No es "el informático"!!!
- Responsable de los servicios
  - Primer nivel: gerencia o similar
  - Segundo nivel: direcciones de área o jefaturas de servicios
- Responsable de seguridad de la información
  - Independiente del Área TIC
- Responsable de los sistemas
  - ATIC

Proyecto de adecuación al ENS

1. Fase PLAN

- **Elaboración y revisión de normativa**
- **Definición de roles y asignar personas**
- **Valorar y categorizar el sistema**

- **Categoría del sistema de información:**
  - Bajo
  - Medio

CATEGORIZAR SISTEMA

La categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectase a la seguridad de la información tratada o de los servicios prestados para:

a) Alcanzar sus objetivos.
b) Proteger los activos a su cargo.
c) Garantizar la conformidad con el ordenamiento jurídico.

Considerando las dimensiones de seguridad:

- Confidencialidad
- Integridad
- Trazabilidad
- Autenticidad
- Disponibilidad

CATEGORIZAR SISTEMA

CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE INFORMACIÓN Y SERVICIOS				
	No Adscrito (N/A)	**BAJO**	**MEDIO**	**ALTO**
Pérdidas económicas	COM.ECO.N No implica pérdidas económicas	COM.ECO.B Pérdidas económicas apreciables (inferior a un 4% del presupuesto anual de la organización)	COM.ECO.M Pérdidas económicas importantes (igual o superior a un 4% e inferior a un 10% del presupuesto anual de la organización)	COM.ECO.A Pérdidas económicas o alteraciones financieras significativas (igual o superior a un 10% del presupuesto anual de la organización)
Reputación	COM.REP.N No implica daño reputacional	COM.REP.B Daño reputacional apreciable con los ciudadanos o con otras organizaciones	COM.REP.M Daño reputacional importante con los ciudadanos o con otras organizaciones	COM.REP.A Daño reputacional grave con los ciudadanos o con otras organizaciones
Protestas	COM.PRO.N No se prevé que pueda desembocar en protestas.	COM.PRO.B Múltiples protestas individuales.	COM.PRO.M Protestas públicas (alteración del orden público)	COM.PRO.A Protestas masivas (alteración seria del orden público)
Delitos	COM.DEL.N No facilitaría la comisión de delitos ni dificultaría su investigación.	COM.DEL.B Favorecería la comisión de delitos	COM.DEL.M Favorecería significativamente la comisión de delitos o dificultaría su investigación.	COM.DEL.A Incitaría a la comisión de delitos, constituiría en sí un delito, o dificultaría enormemente su investigación.

Proyecto de adecuación al ENS

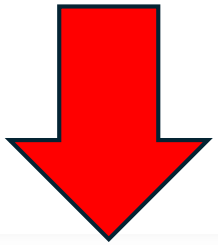
1. Fase PLAN

- Elaboración y revisión de normativa
- Definición de roles y asignar personas
- Valorar y categorizar el sistema
- Análisis de riesgos

- **Herramientas del CCN**
  - https://www.ccn.cni.es/index.php/es/soluciones

ANÁLISIS DE RIESGOS

Hacer cada año



Análisis y Gestión de Riesgos

Informe de Estado de Seguridad en el ENS

Indicadores relacionados para informar de la situación

Almacenamiento en la nube

Sistemas de Gestión Federada de Tickets

Análisis avanzados de ficheros

Gestión de eventos e información de seguridad

Proyecto de adecuación al ENS

1. Fase PLAN

- Elaboración y revisión de normativa
- Definición de roles y asignar personas
- Valorar y categorizar el sistema
- Análisis de riesgos
- Declaración de aplicabilidad

DECLARACIÓN APLICABILIDAD

- **Aplica/No aplica** cada control del ENS, en función de la categoría del sistema.
- **Medidas compensatorias** si no se puede cumplir estrictamente un control obligatorio, incluyendo medidas equivalentes a las exigidas.
- **Firmada** por el responsable de seguridad de la información.

Proyecto de adecuación al ENS

2. Fase DO

- **Implantar, operar y monitorizar el sistema**

Cumplimiento de los controles ENS

- Nivel de madurez:
  - **L0 Inexistente**
  - **L1 Inicial**
  - **L2 Repetible (intuitivo)**
  - **L3 Definido**
  - **L4 Gestionado y medible**
  - **L5 Optimizado**

Mejora continua

Sistema de métricas

Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general.

Verificación del cumplimiento basado en CMM (Capability Maturity Model), Carnegie Mellon University, CMU. A cada cláusula o control evaluado se le asocia uno de los niveles que se detallan a continuación:

Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver. No se está aplicando en este momento.

Cuando la organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas. Los procedimientos son inexistentes. No existen plantillas definidas a nivel corporativo

Cuando existe un mínimo de planificación que, acompañada de la buena voluntad de las personas proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Se normalizan las buenas prácticas en base a la experiencia y al método, pero es impredecible el resultado si se dan circunstancias nuevas. No hay comunicación formal sobre procedimientos y estándares, por lo que las responsabilidades quedan a cargo de cada individuo, dependiendo el resultado de las diferentes acciones del grado de

Proyecto de adecuación al ENS

3. Fase CHECK

- **Auditar. Comprobar cómo estamos y, en su caso, certificarnos.**

Categoría BASICA:

- Autoevaluación de cumplimiento
- Auditoría

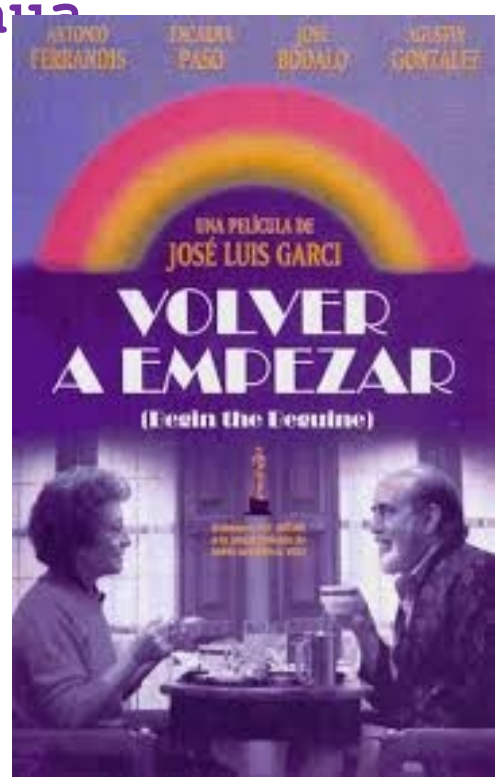
Categoría MEDIA:

- Auditoría interna
- Auditoría de certificación (2 años)

Proyecto de adecuación al ENS

4. Fase ACT

- **Proceso de mejora continua**



Desafíos de la transformación digital en las Administraciones locales: ciberseguridad e inteligencia artificial

Segovia, 11 de abril de 2024

Muchas gracias por su atención

Juan Trastoy

Responsable de Seguridad de la Información

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

juan.trastoy@us