CloudCERT

Testbed Framework to Exercise Critical Infrastructure Protection

indra

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

EUROPE *for business*

INTECO Instituto Nacional de Tecnologías de la Comunicación

Fondazione ICSA

Zanasi & Partners

CONTACTO

http://cloudcert.european-project.eu
info@cloudcert.european-project.eu

http://es.wikipedia.org/wiki/CloudCERT

RESULADOS DEL PROYECTO CLOUDCERT - ENTORNO DE PRUEBAS PARA LA REALIZACIÓN DE EJERCICIOS DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Edita:
Instituto Nacional de Tecnologías de la Comunicación S.A.
INTECO
Avenida José Aguado, 41- 24005 León. España
+34 987 877 189
www.inteco.es

Edición 2013

Versión electrónica disponible en:
http://cloudcert.european-project.eu/

ÍNDICE

1. ANTECEDENTES Y MOTIVACIÓN 4
   - 1.1. Revisión del programa 5
   - 1.2. Motivación 5
   - 1.3. Alcance 5

2. DESCRIPCIÓN DEL PROYECTO 7
   - 2.1. Participantes 8
   - 2.2. Objetivos 9
   - 2.3. Beneficios 9
   - 2.4. Beneficiarios 9
   - 2.5. Dimensión Europea del proyecto y hoja de ruta 10

3. PAQUETES DE TRABAJO 8
   - 3.1. Introducción 14
   - 3.2. WP1. Gestión del Proyecto 15
   - 3.3. WP2. Diseño de la plataforma 16
   - 3.4. WP3. Estándares de información y comunicación 20
   - 3.5. WP4. Definición del marco de seguridad 23
   - 3.6. WP5. Desarrollo 26
   - 3.7. WP6. Experimentación 28
   - 3.8. WP7. Difusión 31

4. SOLUCIÓN TECNOLÓGICA 34
   - 4.1. Plataforma colaborativa 35
   - 4.2. Ciclo de vida del contenido 37
   - 4.3. Ciclo de vida de las vulnerabilidades 38
   - 4.4. WikiPIC 39
   - 4.5. Foro 40
   - 4.6. Servicio de Boletines 41

ANTECENTES y MOTIVACIÓN

DESCRIPCIÓN DEL PROGRAMA

La seguridad y la economía de la UE, así como el bienestar de sus ciudadanos, dependen de ciertas infraestructuras y de sus servicios prestados. La destrucción o la interrupción de ciertas infraestructuras estratégicas podrían suponer la pérdida de vidas, la pérdida de la propiedad y un colapso de la confianza pública en la UE.

2004 Para mitigar esta vulnerabilidad, el Consejo solicitó en 2004 el desarrollo de un Programa Europeo de Protección de Infraestructuras Críticas (PEPIC). Desde entonces, se ha realizado un trabajo de preparación integral, que incluye la organización de seminarios, la publicación de un Libro Verde, los contactos con los actores públicos y privados y la financiación de un proyecto piloto.

2006 El 12 de diciembre de 2006, la Comisión adoptó la Comunicación sobre el PEPIC, que establece un marco global horizontal para las actividades de protección de las infraestructuras críticas en la UE. El Programa propuesto de la UE sobre "Prevención, preparación y gestión de las consecuencias del terrorismo y otros riesgos de seguridad relacionados" se adoptó el 12 de febrero de 2007.

2008 La Directiva 2008/114/CE del Consejo sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección estableció un procedimiento para la identificación y designación de infraestructuras críticas europeas, proporcionando un enfoque común para evaluar estas infraestructuras, con el fin de protegerlas y así adaptarse mejor a las necesidades de los ciudadanos.

2009 Por último, el 30 de marzo de 2009, la Comisión adoptó la Comunicación sobre la Protección de las Infraestructuras Críticas de Información [COM (2009) 149], que indica los principales desafíos que se enfrentan las infraestructuras estratégicas y propone un plan de acción destinado a aumentar su protección.

HOME/2010/CIPS/AG/20

El Programa de la UE sobre "Prevención, preparación y gestión de las consecuencias del terrorismo y otros riesgos de seguridad relacionados" pretende fomentar el intercambio de conocimientos y buenas prácticas entre los distintos agentes responsables de la gestión de crisis y para organizar actividades conjuntas para mejorar la coordinación entre los servicios competentes.

Anualmente, la Comisión Europea elabora programas de trabajo para cubrir las prioridades. Estos programas incluyen las convocatorias de propuestas con el objeto de subvencionar aquellos proyectos que contribuyan a la consecución del programa y los objetivos específicos.

Como resultado de esta convocatoria del programa de 2010, este proyecto "**CloudCERT**" fue seleccionado como uno de los proyectos adjudicatarios.

MOTIVACIÓN

Como se indica en PEPIC, los interesados deben compartir la información sobre el Protección de Infraestructuras Críticas (PIC), en particular sobre medidas relativas a la seguridad de infraestructuras críticas y sistemas protegidos, los estudios de interdependencias y vulnerabilidades relativas a la PIC, amenazas y riesgos. Al mismo tiempo, debe existir garantías de que la información compartida de naturaleza privada, personal o confidencial no se revele y que el personal que manipula la información confidencial será sometido a un adecuado control de seguridad por su Estado miembro.

Para resolver esta necesidad real, el proyecto CloudCERT tiene por objeto la prestación de este entorno de pruebas seguro de intercambio de información con el fin de ejercer funciones de coordinación unificadas, haciendo uso de de protocolos de comunicación comunes estándar para mejorar la visibilidad y concienciación de amenazas, vulnerabilidades comunes, avisos y alertas específicas para el PIC.

Con el fin de lograr este objetivo, es necesario realizar una importante esfuerzo basado en el modelado conceptual y la arquitectura de comunicación de CSIRTs; la definición de intercambio seguro de información, estándares de información y definición de protocolos, el diseño y desarrollo de la plataforma de entorno de pruebas y finalmente, la simulación sobre piloto basado en escenarios y casos de uso.

El alcance de este proyecto se limita a la creación de un piloto de la plataforma CloudCERT para intercambiar información sobre PIC. Por lo tanto, sólo cubre la primera fase de la hoja de ruta establecida.

La plataforma final es un piloto en funcionamiento, con una comunidad de usuarios e información suficientemente útil para probar su funcionalidad y para simular el intercambio de información sobre PIC.

La plataforma permite el intercambio de medidas operativas para la PIC, metodologías, experiencias y conocimientos entre los usuarios que actúan, a través de un repositorio de información, incluyendo al menos los siguientes tipos de información relacionados con PIC:

- Vulnerabilidades.
- Notas, avisos y alertas.
- Amenazas y riesgos.
- Noticias.
- Buenas prácticas.
- Lecciones aprendidas.

La plataforma CloudCERT se basa técnicamente en una aplicación web con gestión de usuarios, incluyendo una fuerte autenticación y con un intercambio seguro de información conforme a normas de interoperabilidad.

DESCRIPCIÓN DEL PROYECTO

PARTICIPANTES

COORDINADOR

- INTECO – Instituto Nacional de Tecnologías de la Comunicación.

CO-BENEFICIARIOS

- CNPIC - Centro Nacional para la Protección de las Infraestructuras Críticas.
- Europe for Business.
- Fondazione ICSA (Intelligence Culture and Strategic Analysis).
- Indra Sistemas.
- INTECO - Instituto Nacional de Tecnologías de la Comunicación.
- Zanasi & Partners.

PRINCIPALES USUARIOS

- INTECO - Instituto Nacional de Tecnologías de la Comunicación.
- CNPIC - Centro Nacional para la Protección de las Infraestructuras Críticas.

INTECO Instituto Nacional de Tecnologías de la Comunicación

CNPIC
CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

EUROPE for business

Fondazione ICSA
Intelligence Culture and Strategic Analysis
Cultura dell'Intelligence e Analisi Strategica

indra

Zanasi & Partners

OBJETIVOS

- Disponer de un **entorno de pruebas** para integrar los mecanismos de coordinación y los esfuerzos de los interesados para gestionar eficazmente los activos de riesgos cibernéticos, centrándose en el intercambio de información referente a PIC y sus aspectos de seguridad.
- Asegurar la **mejora de las infraestructuras de la UE** y la comprensión de las relaciones entre sus elementos, la gestión de riesgos y el aseguramiento de las infraestructuras.
- Proporcionar las capacidades necesarias para **eliminar posibles vulnerabilidades** en las infraestructuras críticas mediante la intercambio de información sobre las vulnerabilidades.
- **Gestionar la seguridad** en su conjunto como un proceso unificado de intercambio de información para cuantificar el riesgo, y decidir y aplicar las acciones oportunas para reducirlo el peligro a un nivel definido y a un coste aceptable.
- **Obtener el valor** derivado de la puesta en práctica de intercambio de información a través de ejercicios, midiendo la eficacia de las medidas preventivas y disuasorias, así como la respuesta a los ataques cibernéticos en los sistemas de infraestructuras críticas.
- Emplear e **intercambiar de manera unificada** la información recopilada en las seis fases del ciclo de vida de la PIC con el fin de crear una garantía de soluciones integrales de protección.

BENEFICIOS

El impacto esperado a **corto plazo** es proporcionar a los agentes implicados en PIC con una plataforma de entorno de pruebas diseñado para soportar el intercambio de información de PIC de los Estados miembros, la coordinación y supervisión.

En el **medio plazo** CloudCERT reforzará la cooperación a través de la puesta en producción de la plataforma en un entorno real operativo y contribuirá a la minimización de los obstáculos de cooperación para los operadores de PIC y de las autoridades de protección en diferentes países de Europa.

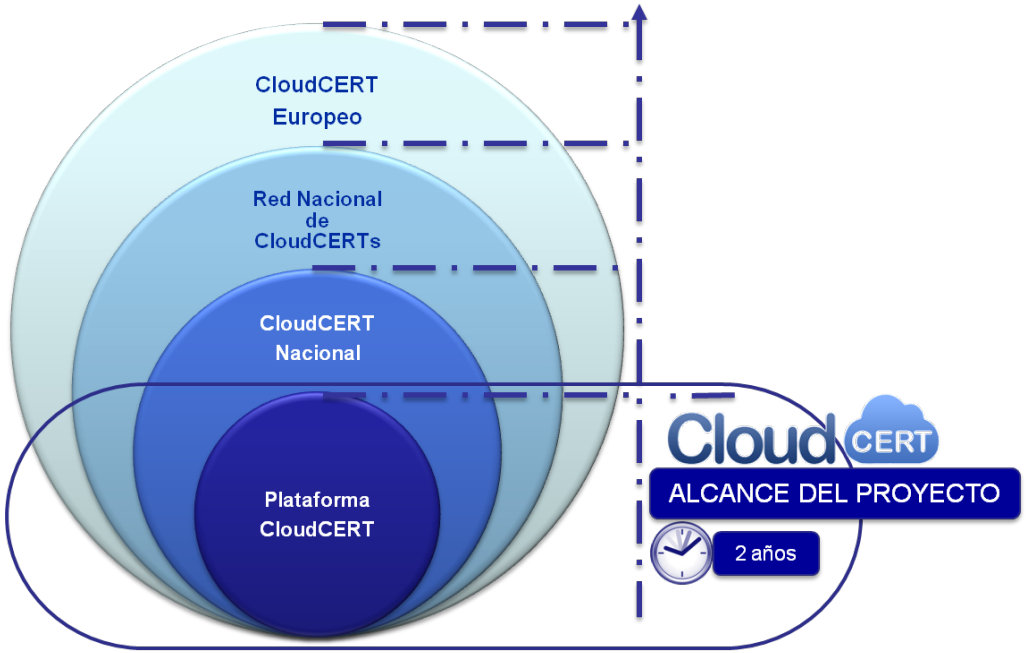
En el **largo plazo**, se espera que contribuya a la creación de un Organismo de Seguridad Europea para la protección de las IC europeas.

BENEFICIARIOS

Los principales grupos destinatarios y beneficiarios de este proyecto son:

- Los Estados Miembros a través de las autoridades de Protección de Infraestructuras Críticas.
- CERTs o CSIRTS con competencias en PIC.
- Los operadores o propietarios de las infraestructuras estratégicas.

DIMENSIÓN EUROPEA DEL PROYECTO Y HOJA DE RUTA



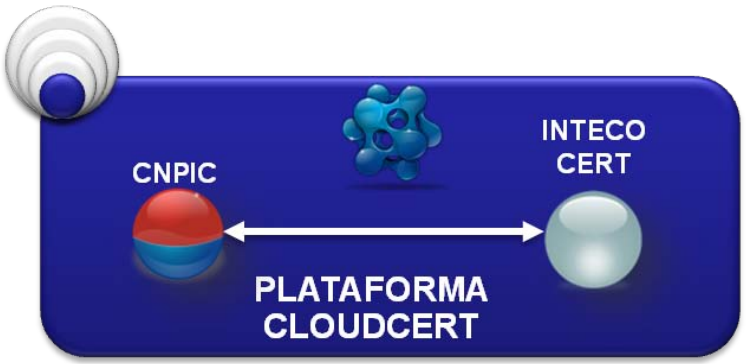
CloudCERT es un **proyecto transnacional,** que implica la participación de al menos tres Estados miembros.

A largo plazo, la hoja de ruta del proyecto consta de las siguientes etapas:

- Plataforma CloudCERT.
- CloudCERT Nacional.
- Red nacional de CloudCERTs.
- CloudCERT Europea.

Para construir una red de colaboración paneuropea, se propone una metodología incremental, generando productos mejorados en cada interacción. Durante la duración del proyecto (2 años) sólo se crea una **plataforma piloto** con el objetivo en mente de construir una red nacional CloudCERT.

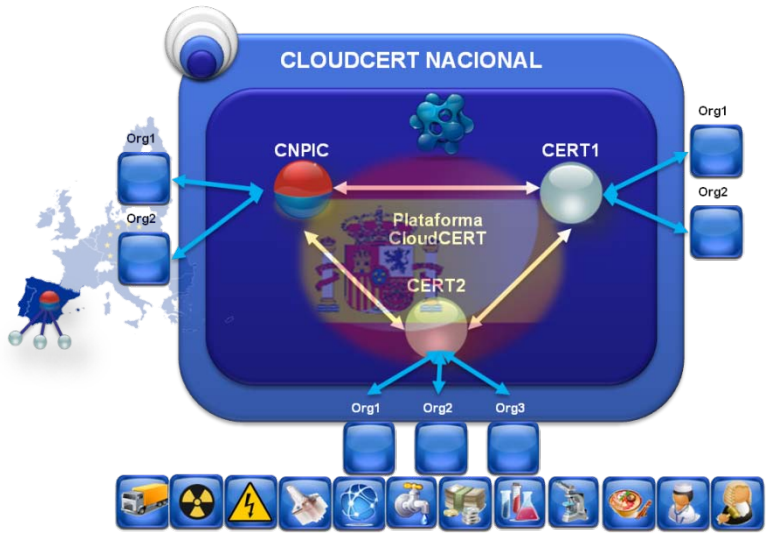
FASE 1 – PILOTO CLOUDCERT (ACTUALMENTE SUVENCIONADO POR LA UE)



En esta primera fase de plan de trabajo, el objetivo es la creación de una plataforma piloto que permita añadir como usuarios de la plataforma, los actores relevantes CIP dentro de un país.

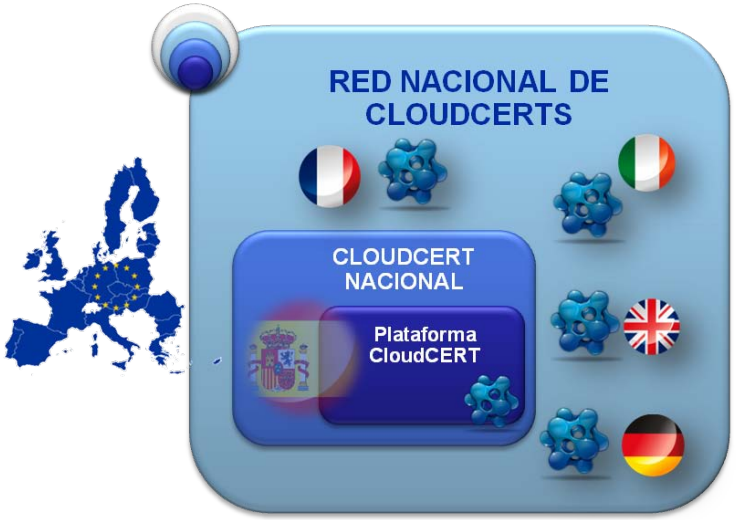
Debido a las limitaciones del proyecto, los usuarios de esta plataforma será tanto el CERT participante en el proyecto (INTECO-CERT), como CNPIC, como Punto Nacional de Contacto PIC.

FASE 2 – CLOUDCERT NACIONAL (OPORTUNIDAD)



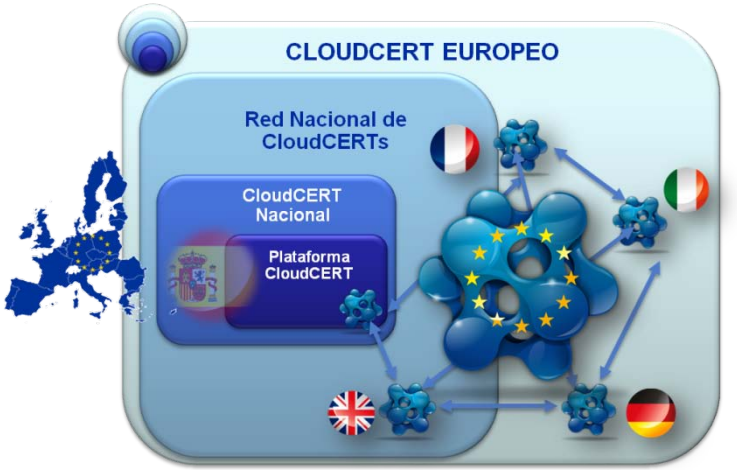
Una vez liberado el piloto, se iniciaría la fase de explotación. Esta etapa comienza con el despliegue de la plataforma en un entorno de producción real con el objetivo de establecer un CloudCERT Nacional que integre el Punto Nacional de Contacto PIC como así como los principales CERTs y otros actores de interés y relevancia en PIC.

FASE 3 – NODOS CLOUDCERT (OPORTUNIDAD)



La etapa siguiente de la hoja de ruta podría ser la réplica en los demás países miembros de la UE para crear nodos de CloudCERT. Las diferencias en el marco regulatorio de cada país pueden condicionar el intercambio de información. Sería deseable añadir condiciones de contorno para adaptar la plataforma, pero no cambiando drásticamente o alterando su propósito principal.

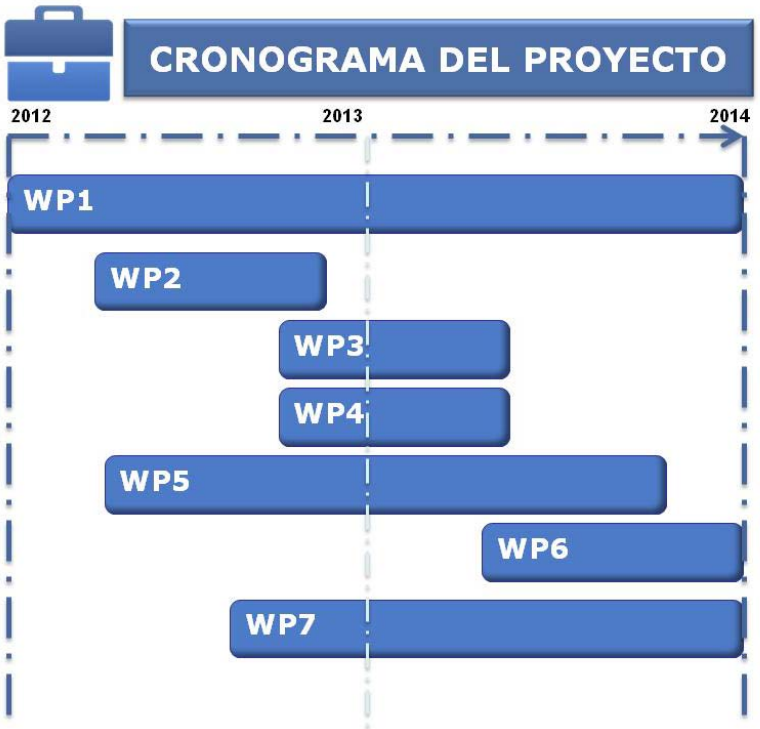
FASE 4 - CLOUDCERT EUROPEO (OPORTUNIDAD)



Si estas etapas de la hoja de ruta tienen éxito, una fase final podría representar la interconexión de los nodos nacionales, formando una red CloudCERT Europea con la suma de todos los miembros nacionales, o una CloudCERT pan-europea entre los Puntos Nacionales de Contacto PIC.

PAQUETES DE TRABAJO

INTRODUCCIÓN



WP1: GESTIÓN DEL PROYECTO

- Coordinación de los socios y los trabajos.
- Gestión de riesgos.
- Gestión económica.

WP2: DISEÑO DE LA PLATAFORMA

- Diseño de la arquitectura del sistema basado en la definición conceptual de la Plataforma CloudCERT.

WP3: ESTÁNDARES DE INFORMACIÓN Y COMUNICACIÓN

- Definición del contenido y formato de la información a ser intercambiada.
- Definición del protocolo para el intercambio de información.

WP4: DEFINICIÓN DEL MARCO DE SEGURIDAD

- Investigación de las prácticas de trabajo actuales para la gestión y el intercambio seguro de información sensible con el objeto de proponer una lista de los requisitos de seguridad.

WP5: DESARROLLO

- Desarrollo de la plataforma que permita un intercambio seguro de información sensible y provea de un catálogo y bases de datos de vulnerabilidades relacionadas con PIC.

WP6: EXPERIMENTACIÓN

- Prueba de la plataforma basada en la definición de escenarios y casos de uso.

WP7: DIFUSIÓN

- Difusión de los resultados del proyecto a través de publicaciones, conferencias, seminarios.

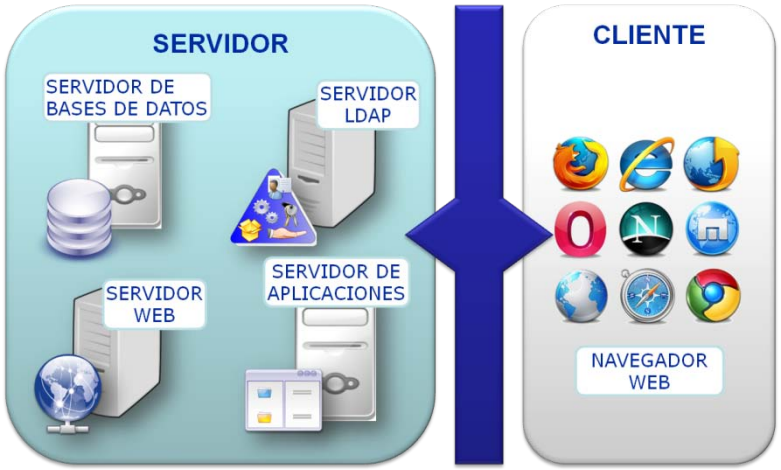
WP1. GESTIÓN DEL PROYECTO

INTECO, como coordinador del Proyecto CloudCERT, es el último responsable de la finalización de todos los paquetes de trabajo y de liderar las actividades de gestión de proyecto.

WP2. DISEÑO DE LA PLATAFORMA

ARQUITECTURA

CloudCERT se basa en una arquitectura cliente / servidor. El modelo de los diferentes componentes de la plataforma CloudCERT se basa en el estándar J2EE.

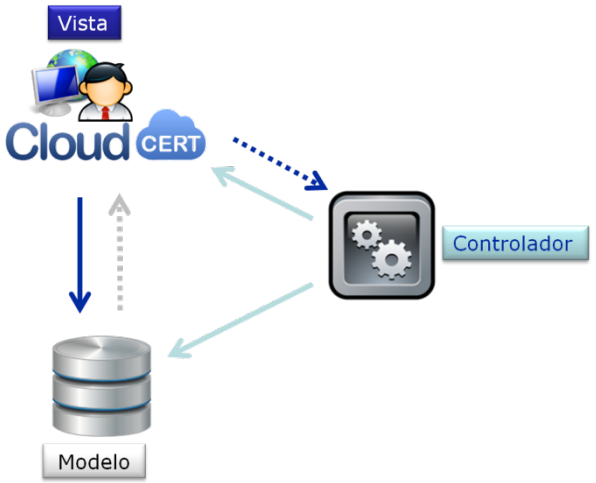


MODELO LÓGICO

Los componentes del modelo lógico de la plataforma se agrupan en los siguientes tipos:

- **Persistencia de datos.** CloudCERT cuenta con un modelo complejo de datos. Para manejarlo, algunos *frameworks* se han utilizado para gestionar el modelo de una manera eficiente.
- **Seguridad a nivel de aplicación.** Todas las tareas relacionadas con la seguridad de la aplicación se basan en la información almacenada en el LDAP.
- **Gestión de flujo de tareas**. CloudCERT utiliza el *framework* Struts. Struts es una marco de apoyo para el desarrollo de aplicaciones Web bajo el patrón MVC en plataformas J2EE.
- **Servicios Web**. Se despliegan en AXIS. AXIS es una implementación SOAP desarrollada por Apache conforme a OASIS y los estándares de W3C.
- **Capa de presentación**. Se basa en el uso de los marcos de trabajo Struts y DWR.

PATRÓN DE DISEÑO MVC

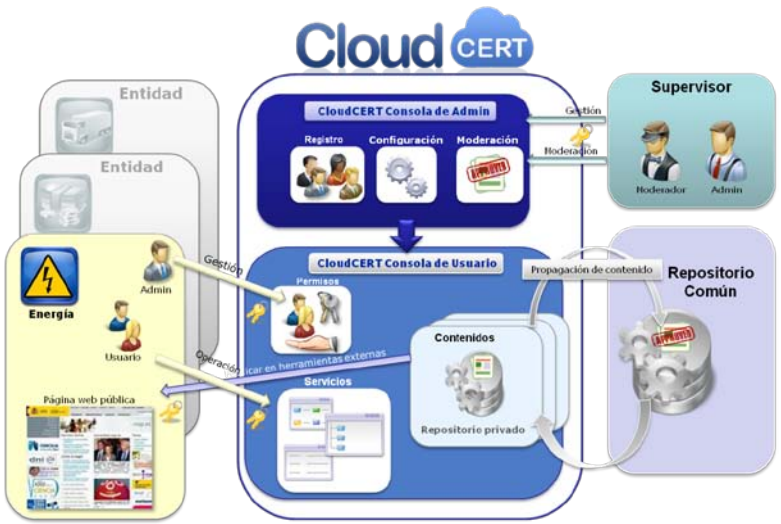


Como la gran mayoría de las aplicaciones J2EE existentes, el Modelo - Vista - Controlador ha sido adoptado en la plataforma CloudCERT.

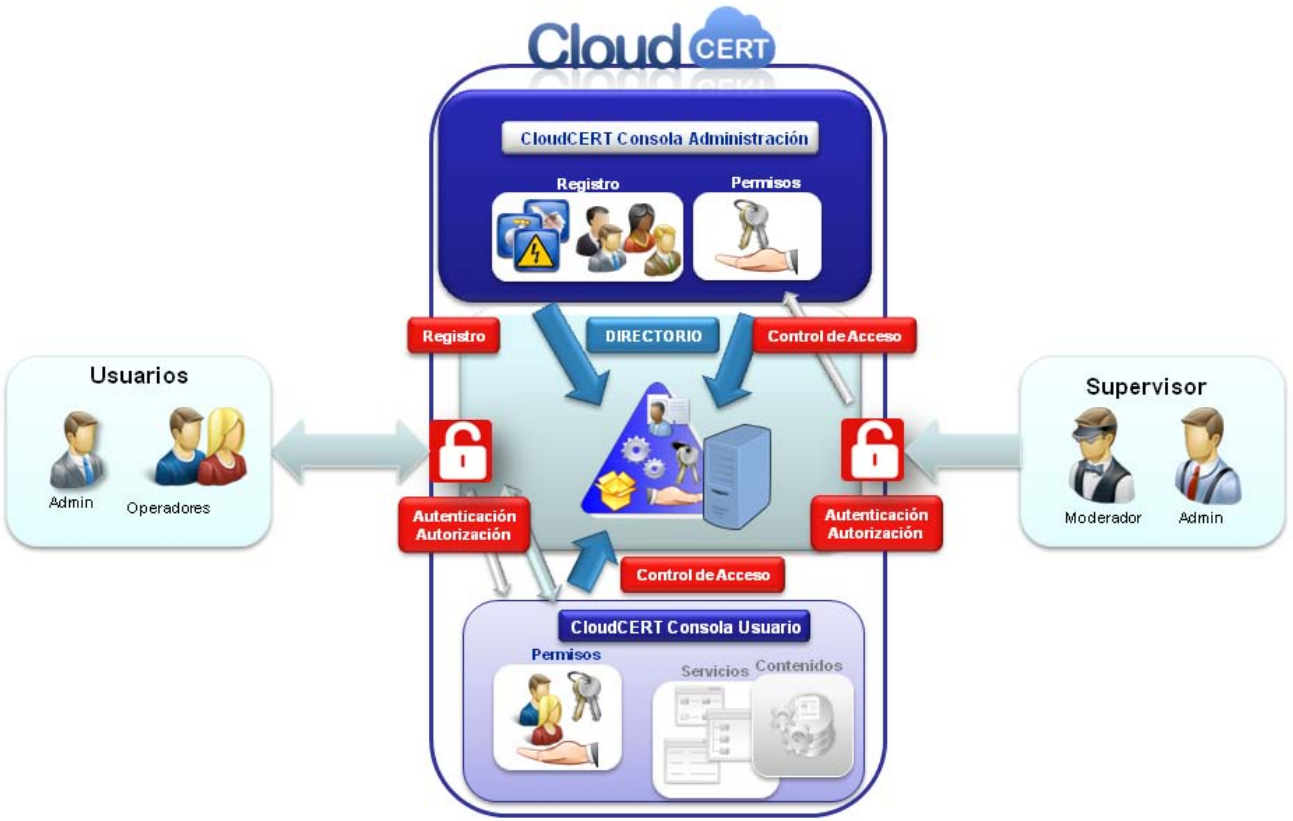
DISEÑO FUNCIONAL

Las aplicaciones y módulos que forman la plataforma CloudCERT incluyen:

- **Módulo de Autenticación CloudCERT**: CAS (Central Authentication Service).
- **Módulo de Gestión de contraseñas**: modulo de gestión de cambio de contraseña y activación de cuentas de usuario.
- **Consola de Usuario CloudCERT**: interfaz de operación y gestión para las distintas entidades.
- **Consola de Administración CloudCERT**: interfaz de gestión y administración de la plataforma CloudCERT (servicios, servicios web, entidades y contenidos).
- **Servicios Web de CloudCERT.**



SEGURIDAD

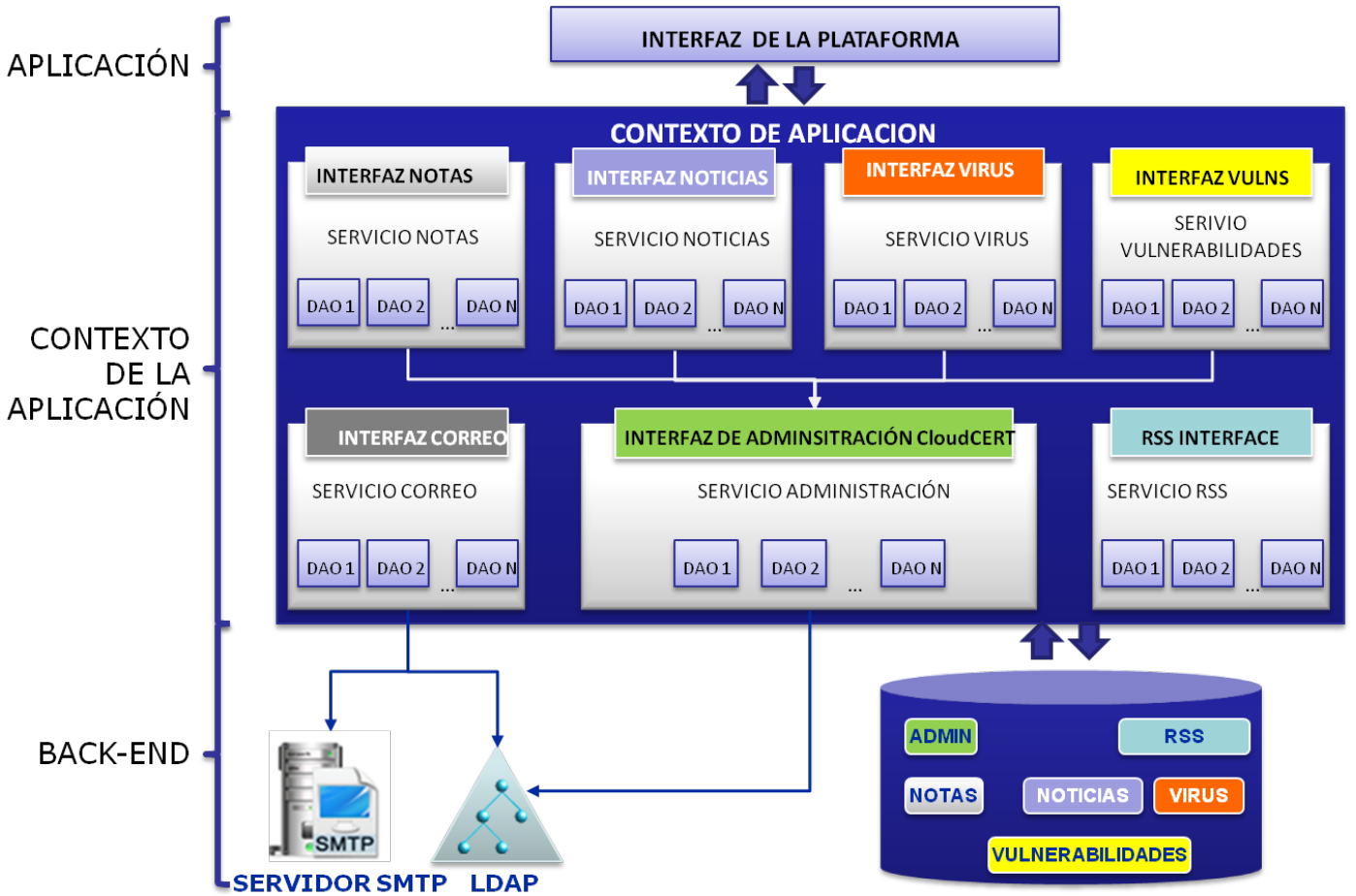


Todas las cuestiones referentes a la seguridad a nivel de aplicación se basan en la información almacenada en LDAP. Los siguientes *frameworks* se han utilizado para administrar la seguridad de CloudCERT:

- **Spring Security.** Módulo perteneciente al *framework* de Spring que permite a la lógica de la aplicación delegar la seguridad, proporcionando mecanismos de autenticación y autorización para las aplicaciones J2EE. Además Spring Security soporta la autenticación en CAS proporcionando una API cliente para interactuar con el servidor CAS.
- **Spring LDAP** perteneciente *framework* de Spring, proporciona mecanismos de interacción para simplificar las operaciones de cualquier tipo de servidor LDAP.

DISEÑO GENERAL

CloudCERT ha definido un contexto global accesible por diferentes aplicaciones, utilizando persistencia de la base de datos y un servidor LDAP:



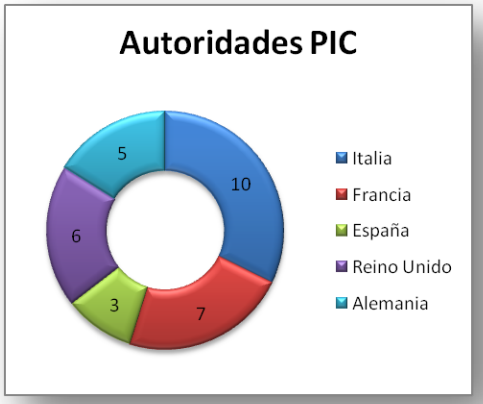
- **Área de aplicación.** Donde se incluye toda la lógica de presentación y flujo de tareas.
- **Área de contexto de aplicación.** El contexto en el que se definen los diferentes servicios que ofrece una interfaz pública a las aplicaciones que soportan u otros servicios.
- **Área Back-End.**
  - Base de datos CloudCERT.
  - LDAP CloudCERT.
  - Servidor SMTP.

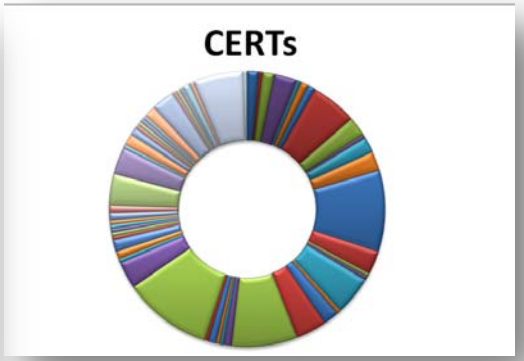
WP3. ESTÁNDARES DE INFORMACIÓN Y COMUNICACIÓN

ONTOLOGÍAS DE CONTENIDOS

- **NOTAS:** administrar y compartir toda la información relacionada con los actos institucionales de las entidades de interés general para la red CloudCERT.
- **NOTICIAS:** introducir, gestionar y compartir todas aquellas noticias públicas que se consideren de interés general.
- **AVISOS:** introducir, gestionar y compartir todos aquellos casos considerados como alertas de especial interés.
- **VIRUS:** introducir, gestionar y compartir todos los virus de especial interés.
- **VULNERABILIDADES:** gestionar y compartir todas aquellas vulnerabilidades de especial interés.
- **CONTENIDOS RSS:** consultar todos esos elementos RSS consideradas como de especial interés.

USUARIOS POTENCIALES DE CLOUDCERT





ESTÁNDARES PARA LA DESCRIPCIÓN E INTERCAMBIO DE INFORMACIÓN

TECNOLOGÍAS DE CARÁCTER GENERAL DE INTERCAMBIO DE INFORMACIÓN

Entre la amplia gama de **protocolos para el intercambio de información** que se han desarrollado a lo largo de los años, tres protocolos se han seleccionado debido a su amplio uso en los diferentes tipos de organizaciones, y a su flexibilidad:

- EDI (*Electronic Data Interchange*).
- XML (*eXtensible Markup Language*).
- SOAP (*Simple Object Access Protocol*).

ESTÁNDARES DE INTERCAMBIO DE INFORMACIÓN ESPECÍFICOS DE SEGURIDAD

El proyecto CloudCERT se centra específicamente en ayudar a los administradores de las infraestructuras críticas y de las infraestructuras de información estratégicas a defenderse mejor frente a ciber amenazas. Los fallos de seguridad son (y seguirán siendo en un futuro próximo) una amenaza para el funcionamiento de las infraestructuras de TI.

Tan pronto como se descubren nuevos fallos, informar a los usuarios y administradores acerca de los problemas identificados se convierte en una tarea de vital importancia tanto para los proveedores de TI y de los equipos de seguridad. La forma más común para circular esta información es por medio de "avisos de seguridad", documentos técnicos que describen en detalle las características del fallo, su impacto potencial, y, a menudo, proporcionan una lista de posibles soluciones.

Esta sección se centra en los **formatos** estándares más populares para los **avisos de seguridad**:

- CAIF (*Common Announcement Interchange Format*).
- EISPP *(European Information Security Promotion Program) Common Advisory Format.*
- DAF *(Deutsches Advisory Format).*
- OpenIOC *(Open Indicators of Compromise).*
- IODEF *(Incident Object Description Exchange Format).*
- VERIS *(Vocabulary for Event Recording and Incident Sharing).*
- STIX *(Structured Threat Information eXpression).*

PLAN DE SOLUCIONES ALTERNATIVO

EVALUACIÓN DE INTERCAMBIO DE CONTENIDOS

Los contenidos que incluyen información acerca de las alertas de especial interés para la red de CloudCERT son adecuados para ser transmitidos mediante el estándar **SOAP** (Simple Object Access Protocol) a través de **HTTPS** (Hypertext Transfer Protocol Secure). Estos son:

- Avisos de Seguridad.
- Virus.
- Vulnerabilidades.

Sin embargo, los siguientes contenidos no son susceptibles de ser intercambiados:

- **Notas**. Este contenido es utilizado por los usuarios de CloudCERT para compartir información relacionada con actos institucionales en su propia plataforma.
- **Noticias**. Este contenido es utilizado por los usuarios de CloudCERT para compartir enlaces URL relacionados con noticias públicas sin ningún interés especial fuera de su propia plataforma.
- **Elementos RSS**. Este contenido es utilizado por los usuarios de CloudCERT para compartir artículos RSS de diferentes fuentes públicas.

INDICADORES

Es importante gestionar cuidadosamente todo el contenido compartido con otras entidades. Para ello, se requiere de un panel de control que permita al administrador monitorizar un conjunto de indicadores relacionados con esta actividad.

Los indicadores susceptibles de ser monitorizados son:

- Número de contenidos producidos durante un período específico de tiempo.
- Número de contenidos leídos durante un período de tiempo especificado.
- Los contenidos más leídos.
- Las entidades productoras más activas.
- Las entidades lectoras más activas.
- Las organizaciones más activas a nivel de importación de contenidos (del repositorio compartido hacia su propio repositorio).
- Distribución mensual de los días más de mayor actividad de producir / consumir contenidos.

WP4. DEFINICIÓN DEL MARCO DE SEGURIDAD

PRÁCTICAS DE TRABAJO PARA LA GESTIÓN SEGURA Y EL INTERCMABIO DE INFORMACIÓN SENSIBLE

La plataforma CloudCERT tiene por objeto facilitar el intercambio de información confidencial sobre PIC a través de diferentes comunidades de interés con todas las garantías de seguridad. De ahí que la primera actividad del paquete de trabajo es una encuesta para investigar sobre las prácticas de trabajo existentes para la gestión segura y el intercambio de información sensible.

SEGURIDAD DE LA INFORMACIÓN

En este capítulo se introduce el dominio de la seguridad de la información y sus principales problemas asociados, centrándose en los Sistemas de Información

- **Confidencialidad**: la divulgación indebida de información debe ser detectada y evitada.
- **Integridad**: la información no debe ser modificada por los usuarios no autorizados.
- **Disponibilidad**: la información debe estar a disposición de los usuarios autorizados cuando sea necesario.

INTERCAMBIO DE INFORMACIÓN PIC

En este capítulo se revisa lo que se ha hecho para permitir el intercambio de información eficaz, dentro del contexto de la PIC, por los gobiernos de dos de los países más destacados en el mundo: los Estados Unidos y el Reino Unido.

CRITICAL INFRASTRUCTURE PROTECTION

Dos países se han tomado como ejemplo y sus planes PIC son analizados y descritos en detalle, Estados Unidos e Italia:

- Estrategia Nacional del departamento *Homeland Security* (EEUU).
- Marco Estratégico Nacional italiano para la seguridad del ciberespacio.

REQUISITOS DE SEGURIDAD DE CLOUDCERT

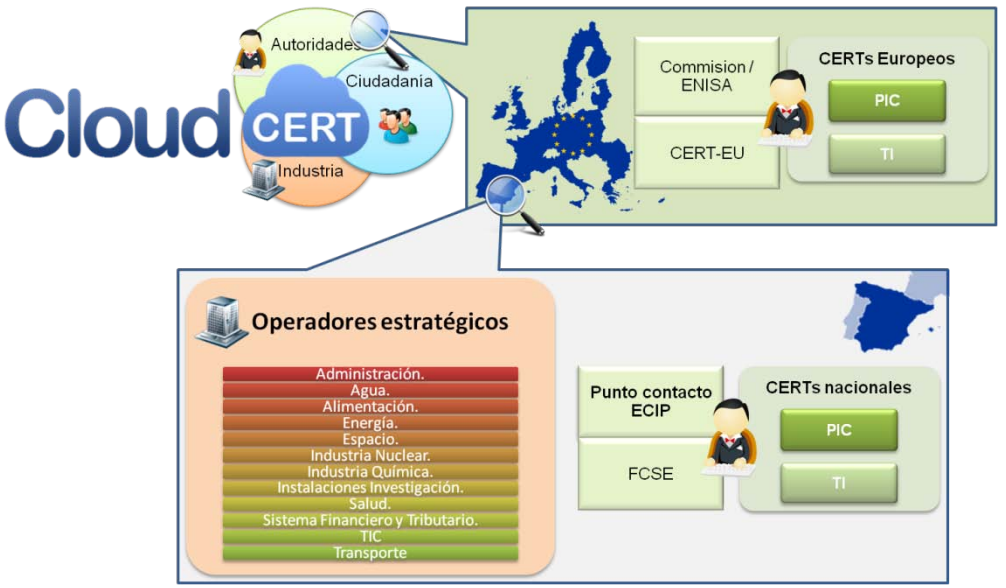
Los objetivos principales de este entregable son:

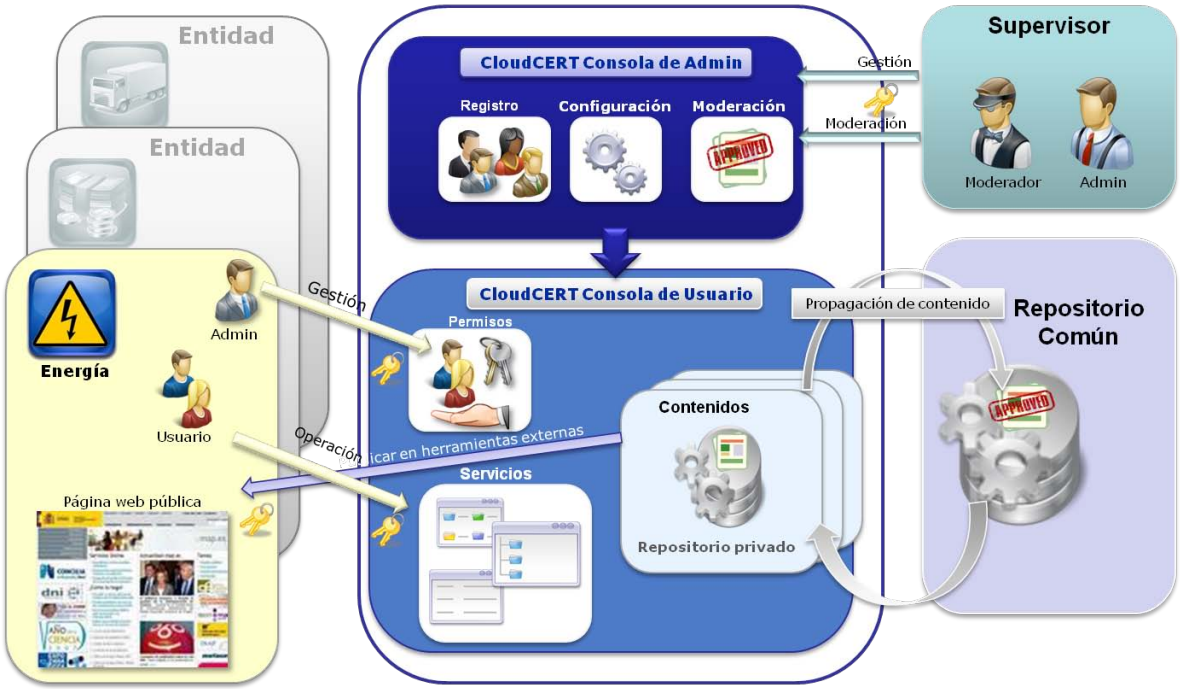
- Identificar las principales fuentes científicas en el campo de la PIC.
- Identificar los métodos y procedimientos que permitan ampliar y fortalecer los procesos de colaboración del sistema.
- Identificar los métodos y procedimientos que permitan ampliar y fortalecer la capacidad de coordinación entre los diferentes actores del sistema a lo largo del ciclo de vida de los contenidos.

Todo ello con el objetivo final de mejorar el modelo de gobernanza con el fin de asignar funciones, responsabilidades y objetivos a los actores del sistema.

Los agentes de CloudCERT están agrupados en tres categorías:

- **Autoridades** (sector público): autoridades competentes en materia de seguridad de la información y la protección de las infraestructuras críticas, incluyendo el nivel legal y operativo. En esto incluye las políticas y los entes reguladores y las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).
- **Industria** (sector privado): operadores estratégicos así como sus principales proveedores (fabricantes de productos y desarrolladores de servicios).
- **Ciudadanía** (publico objetivo): consumidores de los servicios prestados por la infraestructura crítica.



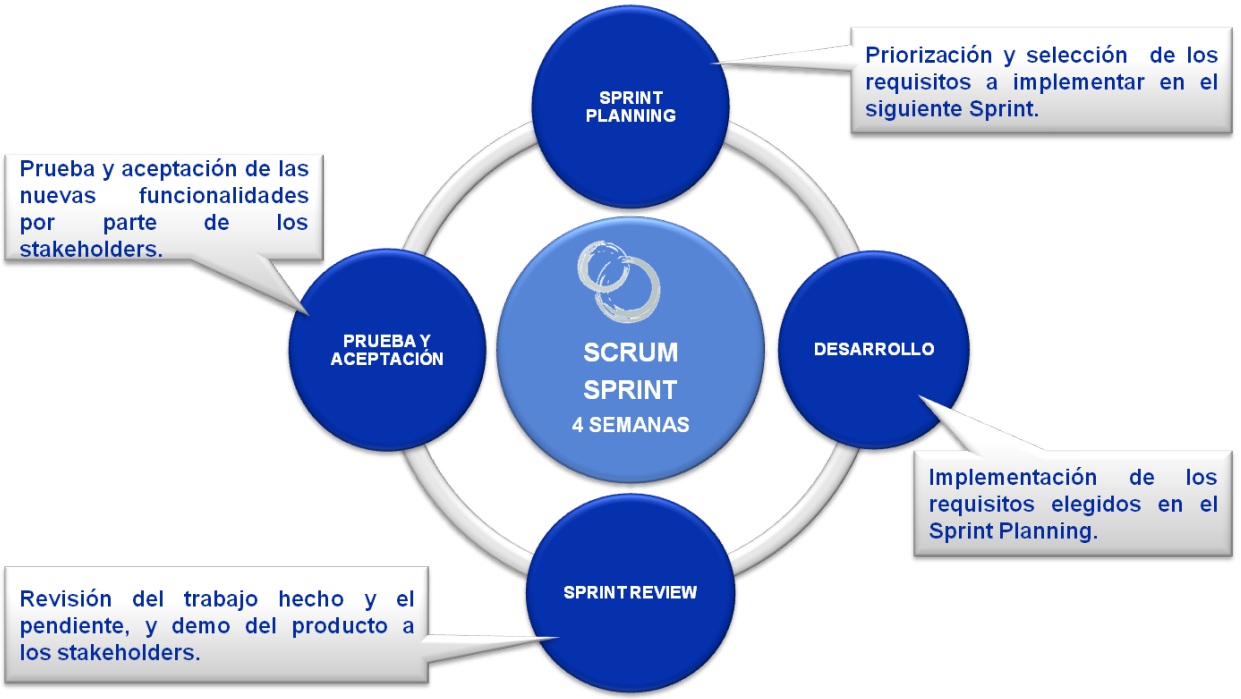


Estos agentes interactúan con la plataforma CloudCERT según el siguiente modelo de gobernanza:

- Diferentes **entidades** pueden acceder a la plataforma: CERTs, FCSE y los operadores estratégicos. Cada entidad tiene su propio espacio para crear contenidos y puede importar contenidos desde el repositorio compartido. Además, pueden exportar automáticamente los contenidos a herramientas externas, como su propio portal web.
- Una entidad **supervisora**:
  - **Administra** la plataforma mediante el registro de las entidades y sus usuarios administradores, así como mediante la configuración y la gestión de los servicios disponibles. El supervisor configura los permisos de acceso a los contenidos y a los servicios contratados
  - **Moderación**. Todos los contenidos que formarán parte del repositorio compartido deben propagarse por el moderador. La moderación también implica publicaciones en herramientas como foros, wiki, etc.
- Cada entidad tiene un **usuario administrador** que puede crear usuarios y asignar permisos para su entidad. Los contenidos del repositorio privado de la entidad pueden ser publicados en un repositorio compartido con la aprobación del supervisor.
- Los **usuarios** pueden interactuar con los contenidos y servicios de la plataforma.

WP5. DESARROLLO

Durante esta fase se lleva a cabo el desarrollo y construcción del piloto. Para este propósito, las siguientes tareas son llevadas a cabo:



ANÁLISIS DE REQUISITOS

La especificación de requisitos de software tiene como objetivos:

- Identificar, solicitando a los usuarios finales, los requisitos y funcionalidades de la plataforma CloudCERT.
- Incorporar los requisitos del marco de seguridad y el intercambio de información confidencial.
- Definir y priorizar las necesidades de la plataforma CloudCERT.

DESARROLLO

A raíz de la metodología ágil Scrum, la fase de desarrollo incluye:

- La aplicación de los requisitos adquiridos en la fase anterior, para crear un piloto funcional.
- Creación de la documentación del usuario y de administración del piloto desarrollado.

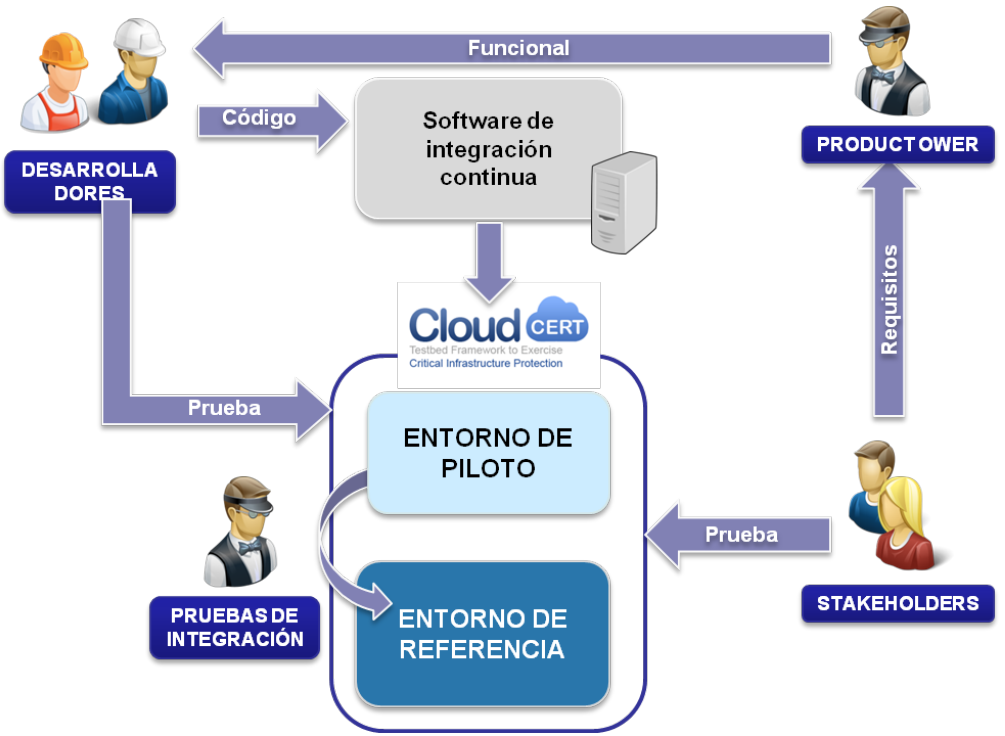
INSTALACIÓN Y CONFIGURACIÓN DE LA PLATAFORMA

Durante esta fase, se proporcionan los entornos de desarrollo y pruebas, y se crean los manuales de instalación y configuración.

ENTORNOS

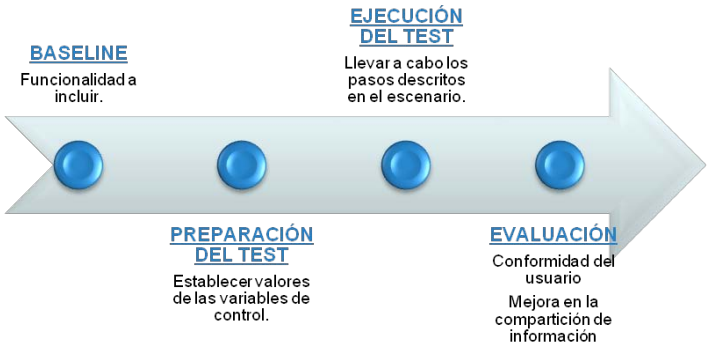
El **entorno piloto** se utiliza para cargar y probar nuevos desarrollos, y para verificarlos después de cada sprint.

Cuando la fase de prueba ha finalizado y todo ha sido verificado, la nueva versión se despliega en el **entorno referencia**, que contiene una versión más estable de la Plataforma CloudCERT.



WP6. EXPERIMENTACIÓN

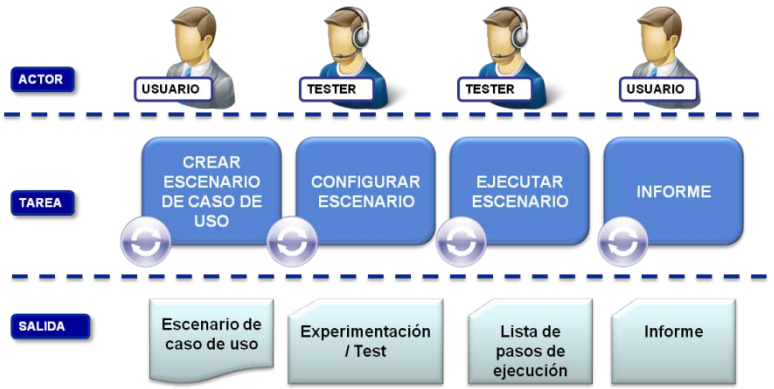
Las actividades del paquete 6 de trabajo se centran en la experimentación y la evaluación en base a ciertos casos de uso de la plataforma piloto desarrollada e instalada en fases anteriores. Las actividades incluyen pruebas funcionales y de aceptación del producto, así como ejercicios de simulación para el intercambio de información entre usuarios de la plataforma para probar y demostrar mediante la simulación, el intercambio de información sobre vulnerabilidades, alertas, avisos de seguridad y reporte de incidentes de seguridad.

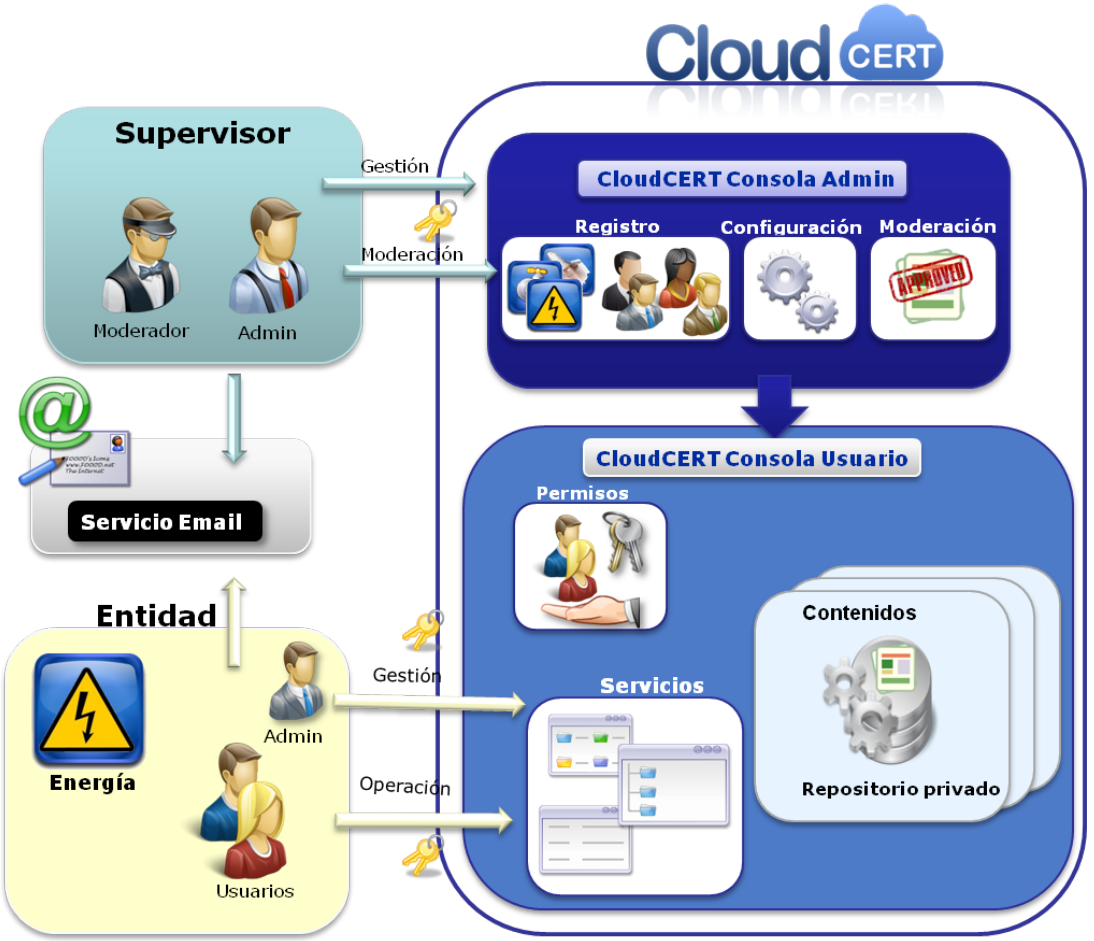


El propósito de la evaluación es simular ciertos escenarios reales para evaluar la contribución de la plataforma CloudCERT para mejorar la colaboración y la cooperación entre los actores PIC en el intercambio de información de la ciberseguridad, y probando de este modo la funcionalidad y los flujos de tareas disponibles.

El objetivo de la evaluación, basada en los resultados de la experimentación, es:

- probar CloudCERT (si los procesos de intercambio de información son soportados correctamente);
- comprobar en qué medida CloudCERT aborda los retos y necesidades del proyecto en términos de colaboración y cooperación;
- y evaluar la mejora potencial habilitada por CloudCERT en el campo de PIC.





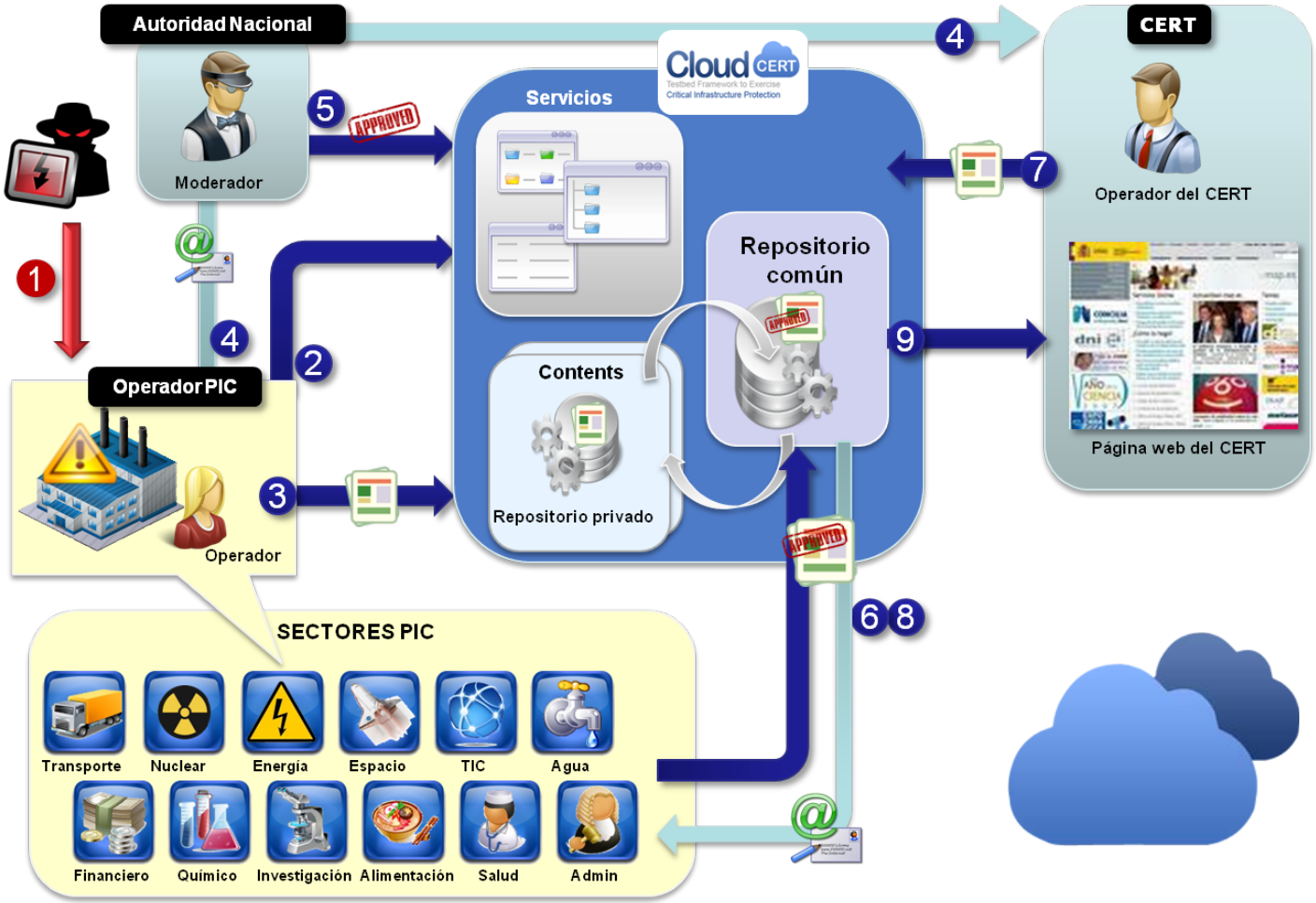
HERRAMIENTAS

- **Consola de Administración.** Permite la gestión integral de las funcionalidades de la plataforma.
- **Consola de Usuario**. Facilita la creación, implementación y operación de nuevas entidades para responder a los incidentes de seguridad.
- **Cliente de correo electrónico.**

ACTORES

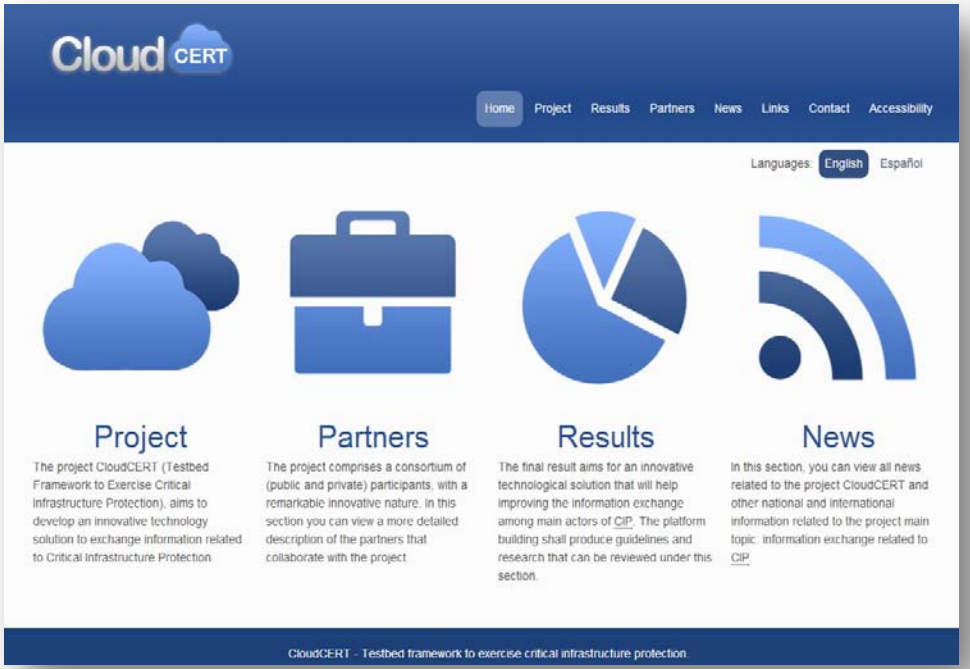
- Usuario – Operador de IC.
- Administrador – Operador de IC.
- Moderador – CERT / Autoridad.
- Administrador- Autoridad.

EJEMPLO DE ESCENARIO DE CASO DE USO



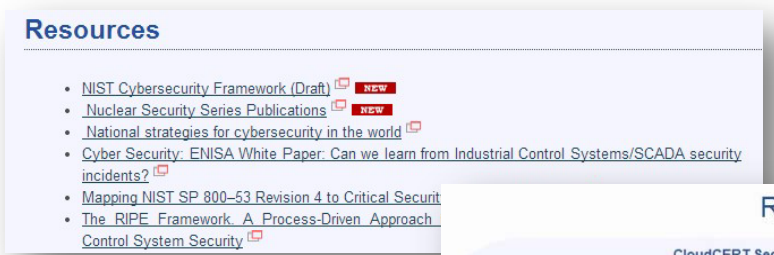
1. Un operador **detecta una vulnerabilidad** en un producto y una intrusión en la red interna.
2. Busca información y lee **procedimiento de gestión de incidentes** en wikiPIC.
3. Crea un **aviso** y escribe en el **foro**.
4. Notifica oficialmente el incidente de seguridad.
5. CNPIC **valida** el aviso.
6. **y 8.** El aviso está visible en CloudCERT y es enviado por correo a través de los boletines.
7. El CERT resuelve el caso y cierra el hilo en el foro escribiendo la solución.
9. El aviso es publicado en el portal web externo.

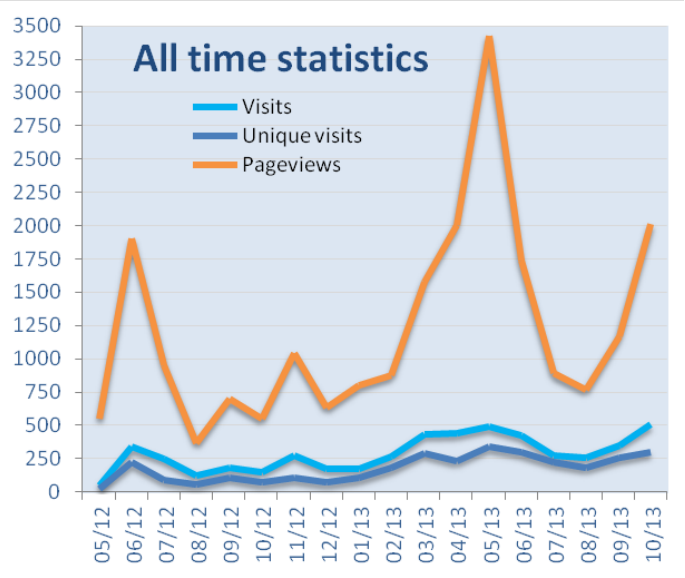
WP7. DIFUSIÓN



Los indicadores más relevantes del portal web del proyecto CloudCERT **http://cloudcert.european-project.eu/** :

- Más de **200** noticias publicadas.
- Más de **5.000** visitas (acumuladas).
- Más de **40** recursos compartidos.
- Más de **22.000** páginas visitadas (acumulado).





WIKIPEDIA

- Español: http://es.wikipedia.org/wiki/CloudCERT
- Inglés: http://en.wikipedia.org/wiki/CloudCERT
- Italiano: http://it.wikipedia.org/wiki/CloudCERT

EVENTOS

2012

- Conferencia CRITIS12 de infraestructuras críticas de información de seguridad. http://critis12.hig.no/

2013

- Semana de la Innovación de Jóvenes Investigadores
- 8º Taller de trabajo de ENISA CERT.

- Protezione delle Infrastrutture Critiche – Telecomunicazioni.

CloudCERT

Testbed Framework to Exercise Critical Infrastructure Protection

Keywords	CERT, CSIRT, Critical Infrastructure Protection (CIP), Critical Infrastructure (CI), Information Sharing, Infrastructure Security
Funding Agency	European Union
Project Type	4rth Annual Work Programme adopted under the Council Decision No 2007/124/EC, Euratom, of Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks for the Period 2007–2013" as part of the General Programme on "Security and Safeguarding Liberties".
Reference	HOME/2010/CIPS/AG/20

FINANCIADO POR LA UE

Innova.- Inteco publica la web del proyecto 'Cloud Cert' sobre protección de infraestructuras críticas

LEÓN, 14 Jun. (EUROPA PRESS) -

El INTECO presenta la web de un consorcio europeo en defensa de las infraestructuras críticas

PROYECTOS

Cloud CERT de INTECO: innovación internacional para la seguridad de las infraestructuras Críticas

CONFERENCIA FINAL

Conferencia final de CloudCERT para difundir los resultados del proyecto europeo para el público objetivo.

- **Fecha:** 22 de noviembre de 2013.
- **Lugar:**
  - Secretaría de Estado para las telecomunicaciones y la sociedad de la información (SETSI). Madrid (España)
- **Público objetivo**
  - Colaboradores del proyecto CloudCERT
  - Operadores españoles de infraestructuras estratégicas, incluyendo los principales fabricantes.
  - Otros CERTs Europeos y organismos competentes en la protección de infraestructuras críticas.
- **Admisión:**
  - Admisión por invitación y retransmitida por video streaming http://www.cloudcert.webcastlive.es.

SOLUCIÓN TECNOLÓGICA

PLATAFORMA COLABORATIVA

¿PUEDE SER CLOUDCERT INTERESANTE PARA USTED?

- Si su organización es un **CERT o un operador de IC,** puede utilizar esta plataforma para gestionar los incidentes de las infraestructuras críticas y compartir información de ciberseguridad.
- Si su organización, **CERT o Autoridad,** es competente en la protección de **los operadores de infraestructuras críticas,** puede obtener una plataforma configurable según sus necesidades para proveer de servicios y herramientas para la protección de las infraestructuras críticas (foro, wiki, etc.)
- Si su organización tiene que interactuar con **las autoridades nacionales PIC,** y en función de sus competencias nacionales puede asignar dentro de la plataforma el rol más adecuado: coordinador, la supervisor, participante, etc.

CONTENIDOS

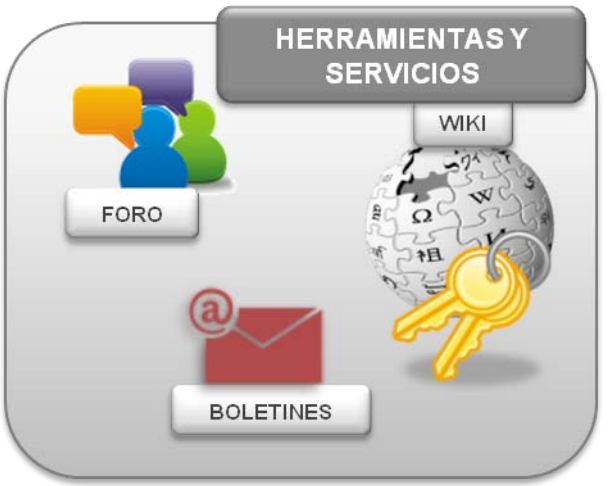
Plataforma CloudCERT le permite crear y propagar contenidos de seguridad, tales como:

- Notas.
- Noticias.
- Avisos.
- Virus.
- Vulnerabilidades.
- Elementos RSS.

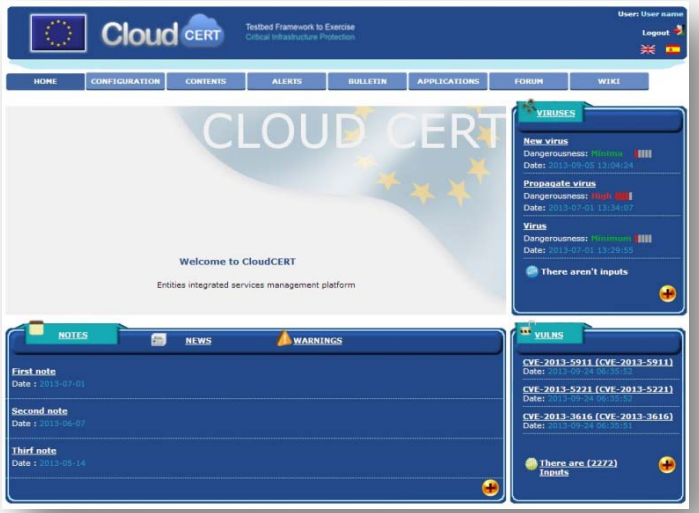
SERVICIOS Y HERRAMIENTAS

La plataforma CloudCERT permite a los usuarios compartir información para prevenir incidentes de seguridad a través de sus servicios:

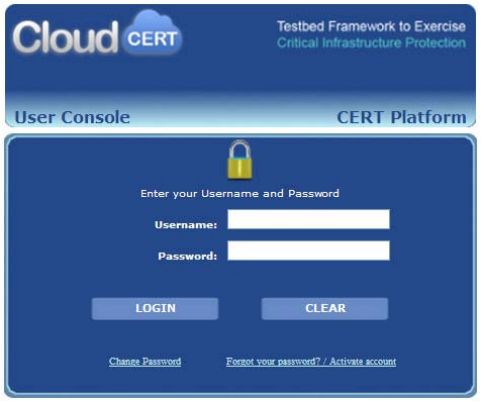
- Foro.
- WikiPIC.
- Servicio de boletines.



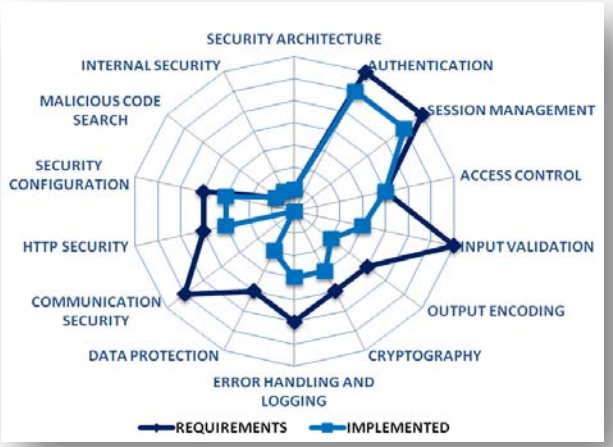
HOJA DE PRODUCTO



- **Plataforma colaborativa** para gestionar de un modo eficiente un repositorio compartido de información sobre ciberseguridad**.**



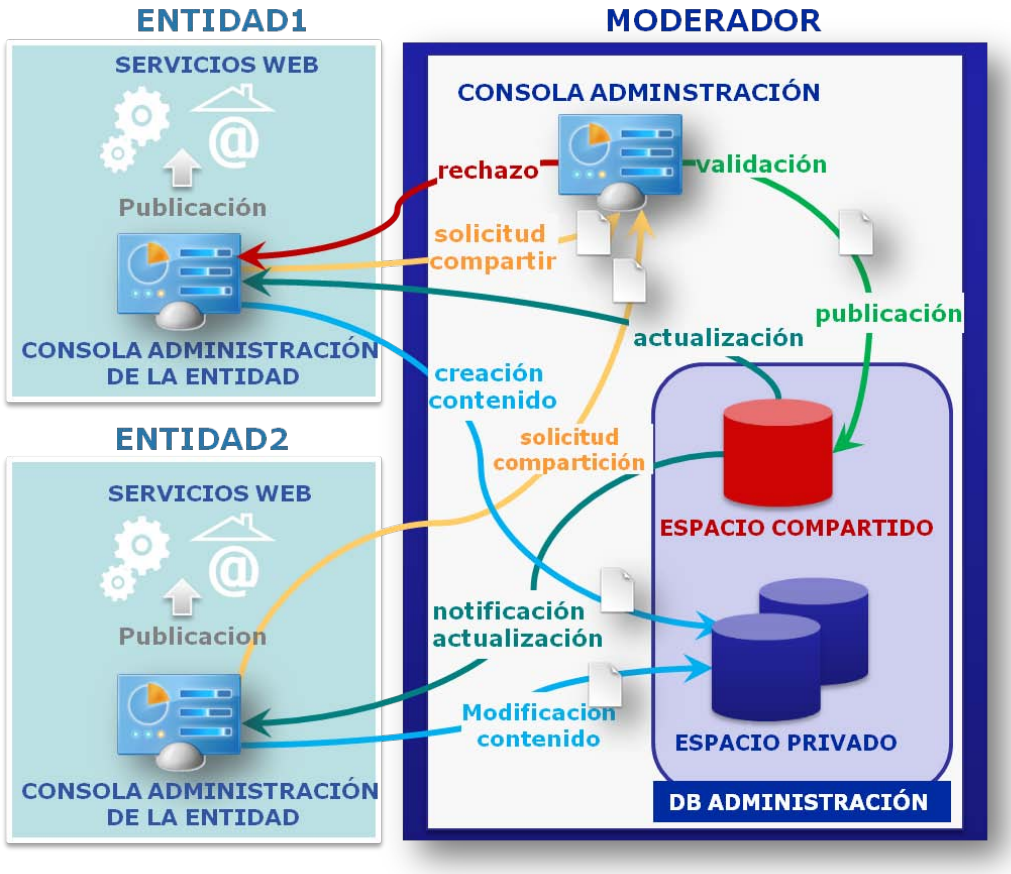
- **Paradigma Cloud** basada en repositorios privados y compartidos.
- Aplicación **multi-idioma** e interfaz de traducción de contenidos.
- **Servicios** personalizados (contratados).
- Plataforma escalable que permite añadir nuevos contenidos, servicios, herramientas y flujos de trabajo.
- **Entorno seguro**:
  - Mecanismo de autenticación basado en nombre de usuario y contraseña: *Central Authentication Service* (CAS).
  - Autorización basada en permisos y roles.
  - Gestión segura de sesiones.
  - Confidencialidad y protección de datos aseguradas.



CICLO DE VIDA DEL CONTENIDO

- CloudCERT permite la **creación** y **actualización** de los contenidos (información estructurada) en forma colaborativa.
- Cada entidad mantiene el contenido en su propio **espacio privado** y podrá solicitar su compartición.
- Un moderador revisa el contenido que se publicará en un **repositorio compartido.**
- Las entidades pueden **recuperar** su contenido para ser publicado en herramientas externas (tales como intranets).

Crear / Modificar un contenido: azul
Solicitud de compartición: amarillo
Actualización contenidos: verde oscuro
Validación de solicitud: verde
Rechazo de solicitud: rojo



Por tanto, el contenido puede encontrarse en los siguientes estados durante su ciclo de vida:

- Creado.
- Modificado.
- Compartido.
- Actualizado.
- Validado.
- Rechazado.

CICLO DE VIDA DE LAS VULNERABILIDADES

- Las vulnerabilidades son un tipo específico de contenido proporcionado a través **de fuentes externas** (como NIST).
- Una tarea programada **importa** automáticamente las vulnerabilidades del sistema.
- El Moderador también puede **solicitar una importación masiva** (para un período de tiempo) en el sistema.
- Las entidades pueden **traducir vulnerabilidades** en su propio espacio privado.

Almacenamiento vulns: azul
Solicitud importación incremental: amarillo
Notificación actualización: verde oscuro
Traducción: verde
Solicitud importación masiva: rojo

Por lo tanto, una vulnerabilidad puede encontrarse en los siguientes estados durante su ciclo de vida:

- Importada.
- Notificada (actualizada).
- Traducida.

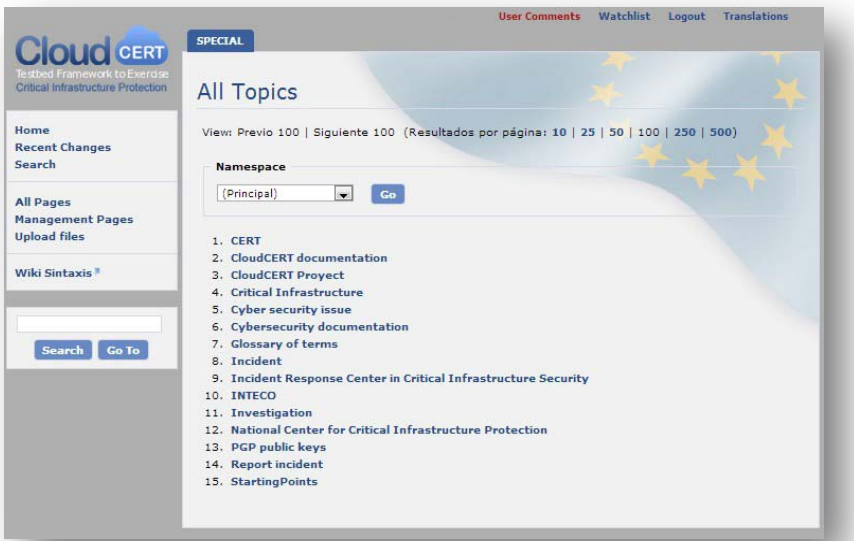
WIKIPIC

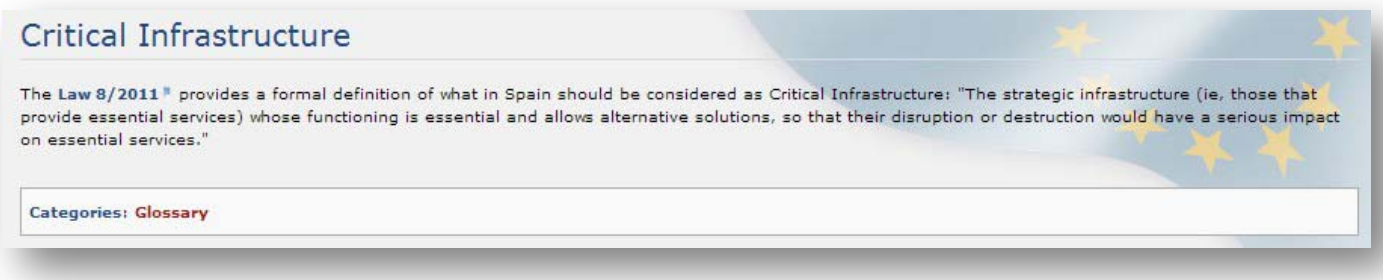
Una wiki es un sistema flexible que permite al administrador definir una jerarquía de páginas. WikiPIC permite el mantenimiento de contenidos no estructurados de un modo colaborativo con los siguientes elementos estructurales:

- **Índice** – Página de índice que muestra enlaces a diferentes páginas de la wiki con una temática similar.
  - **Página** – Páginas individuales sobre un tema específico.

WikiPIC posee la siguiente estructura temática:

- **Documentación CloudCERT**:
  - Presentación genérica del proyecto y los recursos principales.
    - Manual de usuario.
    - Manual de administrador.
    - Manual de desarrollador.
- **Documentación de Ciberseguridad**:
  - Procedimiento operativo de ciberincidentes.
  - Marco legal
  - Enlaces de interés en el ámbito de PIC.
- **Glosario.** Principales términos relacionados con la PIC.

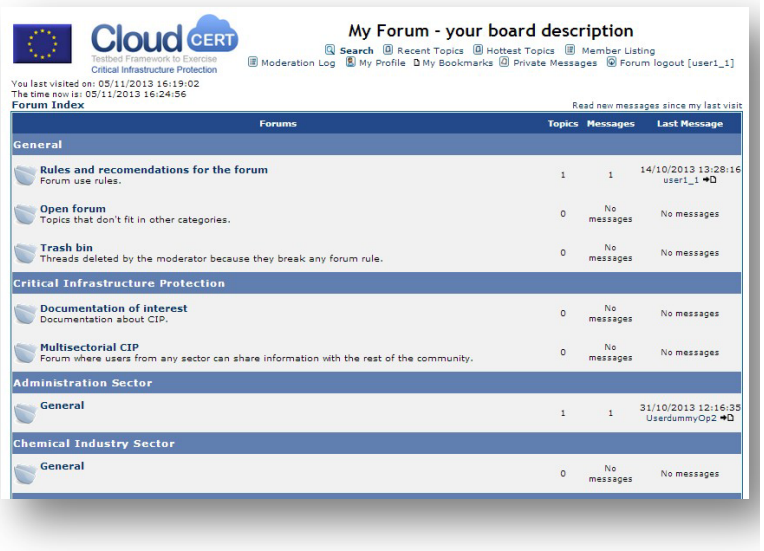




FORO

El servicio de foro permite el intercambio de información no estructurada en base a la siguiente jerarquía:

- **Categoría.** Es el elemento superior de la jerarquía y por lo general utilizado para agrupar varios foros relacionados. Este es un grupo lógico, y un foro siempre dentro de una categoría tiene su propio ciclo de vida.
  - **Foro**. Un foro es un grupo debate sobre el mismo tema.
    - **Tema**. Se trata de la discusión misma, todos aquellos mensajes de los usuarios hablando de un tema específico.



El foro de CloudCERT cuenta con las siguientes categorías:

- **General**. Foros de información general.
- **Protección de infraestructuras críticas.** Donde los usuarios pueden discutir y compartir información general sobre protección de infraestructuras críticas con el resto de la comunidad.
- Todos los operadores de infraestructuras críticas tiene un foro reservado a su **sector** (según la clasificación española), donde los usuarios pueden compartir información con otros actores relevantes en el sector.
  - Administración.
  - Agua.
  - Alimentación.
  - Energía.
  - Espacio.
  - Industria Nuclear.
  - Industria Química.
  - Instalaciones Investigación.
  - Salud.
  - Sistema Financiero y Tributario.
  - Tecnología Información y Comunicaciones.
  - Transporte.

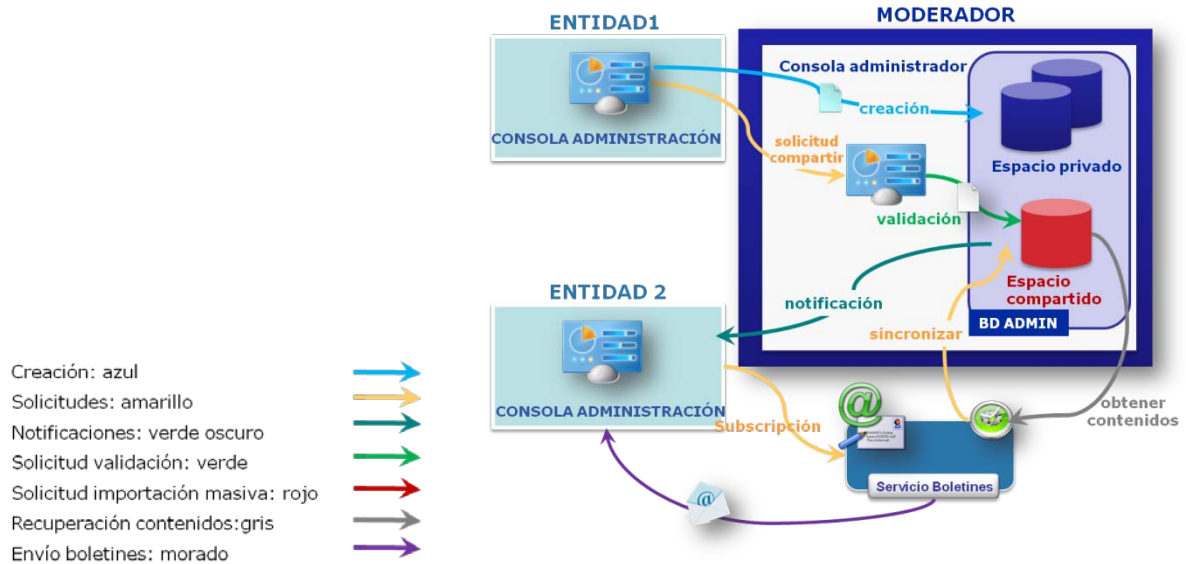
SERVICIO DE BOLETINES

El Servicio de Boletines es un servicio externo que se comunica con la plataforma CloudCERT para **recibir** las **suscripciones de usuarios**, y **obtener los contenidos de seguridad** almacenados en las bases de datos de CloudCERT para crear los boletines. El Servicio de Boletines es responsable de crear y dar formato a los boletines, y enviar los boletines a los usuarios finales de acuerdo con sus preferencias.

Cada entidad registrada CloudCERT, puede suscribir usuarios (usuarios previamente registrados o usuarios externos) a los diferentes boletines de seguridad con el objeto de recibir los boletines periódicamente a sus buzones de correo electrónico.

La suscripción puede ser procesada por el administrador de la entidad o por el usuario final.

- El servicio de boletines permite a los usuarios estar informados acerca de las actualizaciones de contenido a través de notificaciones por correo electrónico.
- Se requiere un proceso de suscripción para seleccionar el tipo de avisos y su contenido.
- El servicio de boletines recopila los contenidos, crea los boletines personalizados y envía el boletín a cada usuario final.



Cloud CERT

Testbed Framework to Exercise
Critical Infrastructure Protection

CloudCERT - Entorno de pruebas para la realización de ejercicios de protección de infraestructuras críticas.

HOME/2010/CIPS/AG/20.
Con la financiación del Programa "Prevención, preparación y gestión de las consecuencias del terrorismo y otros riesgos relacionados con la seguridad". Comisión Europea - Dirección General de Justicia, Libertad y Seguridad