CloudCERT

Testbed Framework to Exercise

Critical Infrastructure Protection

indra

CNPIC

EUROPE for business

INTECO

Fondazione ICSA

Zanasi & Partners

CONTATTO

http://cloudcert.european-project.eu

info@cloudcert.european-project.eu

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

RISULTATI DEL SISTEMA DI VALUTAZIONE CLOUDCERT PER ESERCITARE LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE

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

Versione elettronica disponibile all'indirizzo:
http://cloudcert.european-project.eu/

INDICE

BACKGROUND e MOTIVAZIONE

PANORAMICA DEL PROGRAMMA

La sicurezza e l'economia dell'Unione Europea così come il benessere dei suoi cittadini dipendono da alcune infrastrutture e dai servizi che forniscono. La distruzione o il malfunzionamento di infrastrutture che erogano servizi fondamentali può comportare la perdita di vite, di proprietà, un crollo della fiducia e del morale pubblico nell'UE.

2004 Per contrastare queste potenziali vulnerabilità, il Consiglio Europeo ha richiesto, nel 2004, lo sviluppo di un Programma Europeo di Protezione delle Infrastrutture Critiche (PEPIC). Da quel momento, è stato intrapreso un lavoro propedeutico globale, che includeva l'organizzazione di seminari sull'argomento, la pubblicazione di un Libro Verde, discussioni con attori pubblici e privati e il finanziamento di un progetto pilota.

2006 In quest'ottica, il 12 dicembre 2006, la Commissione ha adottato la comunicazione sul PEPIC, che definisce una struttura orizzontale generale per attività di protezione delle infrastrutture critiche a livello dell'UE. Il programma UE proposto sulla "Prevenzione, preparazione e gestione delle conseguenze in materia di terrorismo e di altri rischi correlati alla sicurezza" è stato adottato il 12 Febbraio 2007.

2008 La Direttiva 2008/114/EC del Consiglio sull'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione, definisce una procedura per individuare e designare le infrastrutture critiche europee (ICE). Allo stesso tempo, fornisce un approccio comune per valutare queste infrastrutture, nell'ottica di migliorarle per salvaguardare meglio le necessità dei cittadini.

2009 Infine, il 30 marzo 2009, la Commissione ha adottato la comunicazione sulla Protezione delle Infrastrutture Critiche dell'Informazione (CIIP) [COM(2009) 149], che descrive nel dettaglio le principali sfide da affrontare nel settore delle infrastrutture critiche dell'informazione e propone un piano d'azione volto ad aumentarne la protezione.

HOME/2010/CIPS/AG/20

Il programma UE sulla "Prevenzione, preparazione e gestione delle conseguenze in materia di terrorismo e di altri rischi correlati alla sicurezza" mira a incoraggiare uno scambio di know-how e buone pratiche fra i diversi agenti responsabili della gestione delle crisi e a orchestrare sforzi congiunti per migliorare il coordinamento fra i dipartimenti pertinenti.

La Commissione Europea elabora programmi operativi annuali per far fronte alle priorità entro ogni anno. Tali programmi includono inviti a presentare proposte per definire sovvenzioni d'azione da elargire a progetti transnazionali e/o nazionali che possano contribuire al conseguimento degli obiettivi generali e specifici del programma. Come risultato dell'invito a presentare proposte del programma 2010, il progetto "**CloudCERT**" è stato scelto fra i progetti vincitori.

MOTIVAZIONE

Come stabilito dal PEPIC, gli attori devono condividere informazioni sulla Protezione delle Infrastrutture Critiche (PIC), in particolare sulle misure che riguardano la sicurezza delle infrastrutture critiche e dei sistemi protetti, gli studi sull'interdipendenza e la valutazione delle vulnerabilità, delle minacce e dei rischi connessi alla PIC. Allo stesso tempo, si deve garantire che le informazioni condivise di natura protetta, sensibile o personale non vengano divulgate pubblicamente e che qualsiasi membro del personale che gestisca informazioni riservate sia soggetto ad un esame accurato delle credenziali da parte del proprio Stato Membro per motivi di sicurezza.

Per rispondere a questa necessità reale, il progetto CloudCERT intende fornire questo sistema di valutazione per la condivisione sicura di informazioni allo scopo di garantire un coordinamento uniforme utilizzando gli stessi standard di protocollo di comunicazione per migliorare la visibilità delle informazioni già note relative alle minacce comuni, vulnerabilità, avvisi e allerta specifici alla PIC.

Per raggiungere quest'obiettivo, è necessario portare avanti un lavoro importante basato sulla modellazione e l'architettura di comunicazione concettuale CSIRT; definizione di condivisione sicura di informazioni; definizione di standard e protocollo di informazione; rogettazione e implementazione della piattaforma di valutazione; e, infine, avviare un progetto pilota per conoscere la situazione reale in base a scenari di casi d'uso.

La portata di questo progetto si limita alla realizzazione della piattaforma pilota CloudCERT. Pertanto, copre soltanto la prima fase della roadmap nel lungo termine.

La piattaforma finale è un modello pilota operativo con una comunità di utenti e informazioni sufficientemente utili da testarne la funzionalità e svolgere esercizi di simulazione per lo scambio di informazioni sulla PIC.

La piattaforma permette lo scambio di misure operative, metodologie, esperienze e know-how sulla PIC fra gli utenti che fungono da archivio di informazioni delle seguenti tipologie:

- Vulnerabilità.
- Note, Notifiche e Allerta.
- Conoscenza delle minacce.
- News.
- Buone Pratiche sulla PIC.
- Conoscenze acquisite sulla PIC.

La piattaforma CloudCERT, dal punto di vista tecnico, si basa su un'applicazione web gestita dall'utente, che offre un sistema di autenticazione solido e uno scambio sicuro di informazioni in base a standard interoperabili.

DESCRIZIONE del PROGETTO

PARTECIPANTI

COORDINATORE

- INTECO - National Institute for Communication Technologies.

COBENEFICIARI

- CNPIC – Centro Nazionale per la Protezione delle infrastrutture Critiche.
- Europe for business.
- Fondazione Intelligence Culture and Strategic Analysis (ICSA).
- Indra Systems, Inc.
- INTECO - National Institute of Communication Technologies.
- Zanasi & Partners.

PARTNER UTENTI

- INTECO - National Institute for Communication Technologies
- CNPIC - Centro Nazionale per la Protezione delle infrastrutture Critiche.

OBIETTIVI

- Fornire un **sistema di valutazione** volto ad integrare i meccanismi per coordinare i partenariati e le attività degli attori, per permettere uno scambio efficace di informazioni sulla PIC e i vari aspetti della sua sicurezza.
- **Salvaguardare le infrastrutture dell'UE**, migliorando la comprensione delle relazioni fra i loro elementi e il legame fra gestione dei rischi e protezione delle infrastrutture.
- Garantire le capacità necessarie per **eliminare le potenziali vulnerabilità** nelle infrastrutture critiche, condividendo le informazioni sulle vulnerabilità.
- **Gestire la sicurezza** in generale utilizzando un processo unificato di scambio di informazioni per determinare i rischi e prevedere e attuare azioni volte a ridurre i rischi ad un livello definito e accettabile, ad un costo accettabile.
- **Ricavare un valore** derivante dallo scambio di informazioni svolgendo esercizi, misurato in base all'efficacia della prevenzione, deterrenza e risposta agli attacchi informatici sui sistemi di controllo all'interno delle infrastrutture critiche.
- Un **sistema comune di segnalazione** e di **scambio di informazioni** nelle sei fasi del ciclo di vita della PIC per proporre una soluzione globale.

VANTAGGI

L'impatto previsto a **breve termine** consiste nel dotare gli organi PIC di una piattaforma di valutazione ideata per supportare lo scambio di informazioni sulla PIC, la supervisione e il coordinamento fra Stati Membri

Nel **medio termine**, CloudCERT rafforzerà la cooperazione attraverso l'implementazione della piattaforma in un ambiente di produzione reale, e contribuirà a ridurre al minimo gli ostacoli alla cooperazione fra operatori PIC e autorità di protezione in diversi paesi europei.

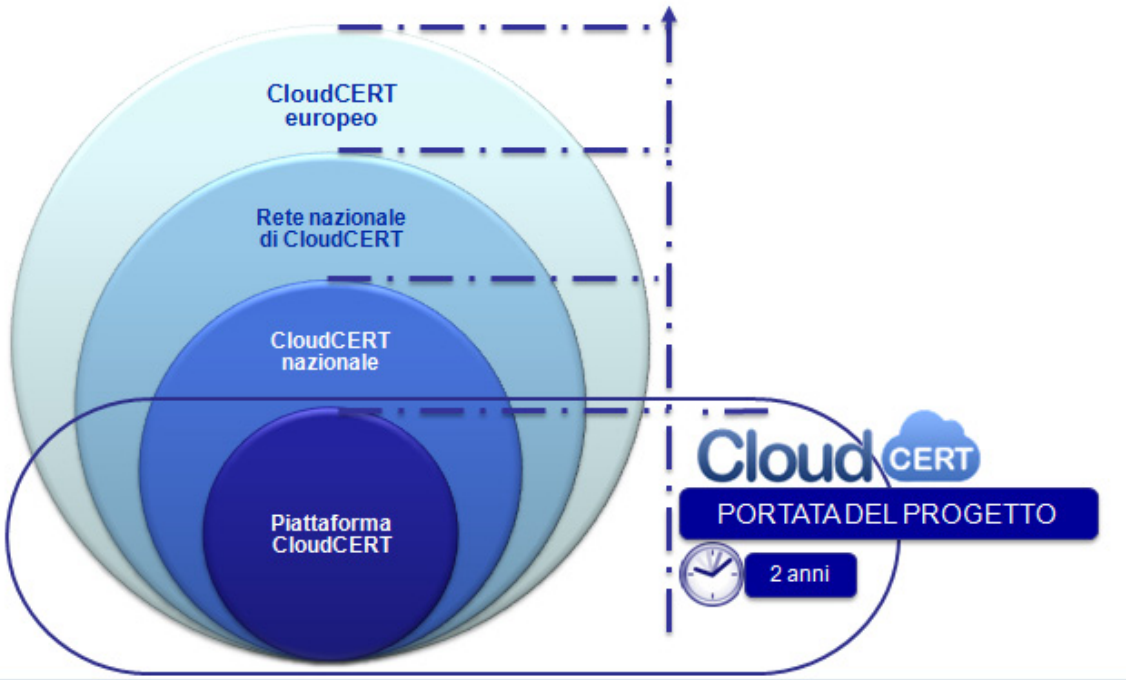
Nel **lungo termine**, si prevede che contribuirà alla creazione di un ambiente di Sicurezza interna Europea per la protezione delle IC europee.

GRUPPI TARGET

I principali gruppi target e beneficiari di questo progetto sono:

- Stati Membri attraverso le autorità di Protezione delle Infrastrutture Critiche.
- CERT o CSIRT competenti in CIP.
- Operatori o Proprietari delle Infrastrutture critiche (IC).

DIMENSIONE EUROPEA E ROADMAP DEL PROGETTO



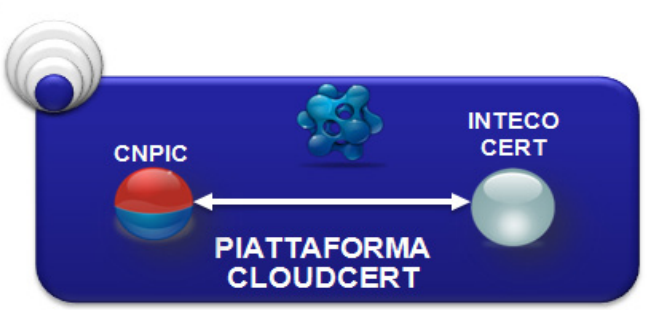
CloudCERT è un **progetto transnazionale**, che coinvolge partner di almeno due Stati Membri.

La strategia del progetto a lungo termine segue una roadmap con le seguenti fasi:

- Piattaforma CloudCERT.
- CloudCERT nazionale.
- Rete CloudCERT nazionale.
- CloudCERT europeo.

Per costruire una rete di collaborazione paneuropea, proponiamo una metodologia basata su approcci incrementali consecutivi che generino prodotti in fasi che miglioreranno durante ogni interazione. Per tutta la durata del progetto (2 anni) si crea solo la **piattaforma pilota**, nell'ottica di costruire un CloudCERT nazionale.

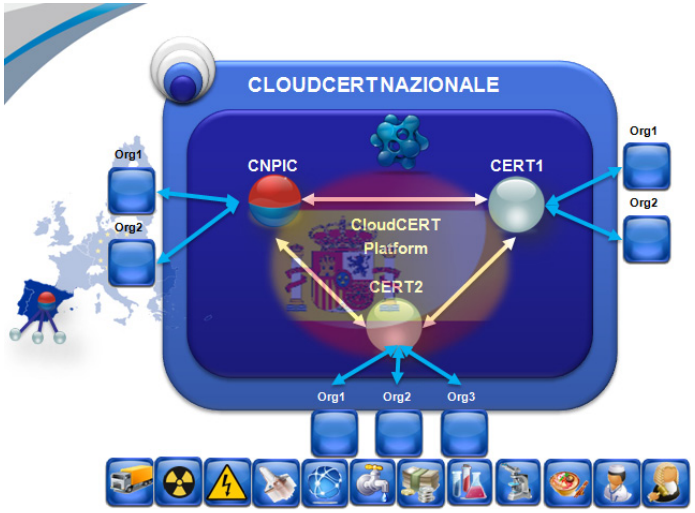
FASE 1 – PROGETTO PILOTA CLOUDCERT (ATTUALMENTE FINANZIATO DALL'UE)



In questa prima fase della roadmap, l'obiettivo è la creazione della piattaforma pilota che permette di aggiungere gli attori della PIC di un paese come utenti.

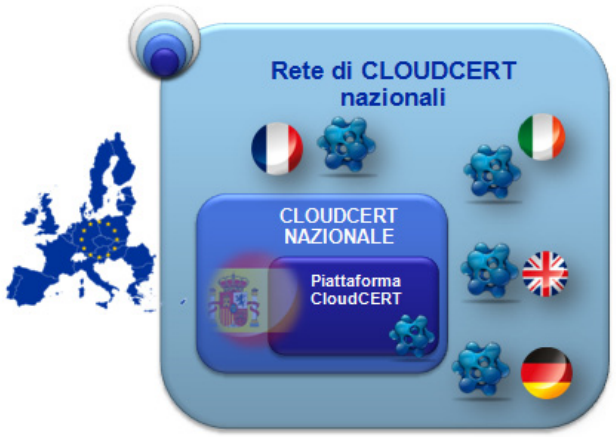
A causa dei limiti del progetto, gli utenti di questa piattaforma saranno i CERT (INTECO-CERT) e i Centri Nazionali PIC (CNPIC) che partecipano al progetto.

FASE 2 - CLOUDCERT NAZIONALE (OPPORTUNITÀ)



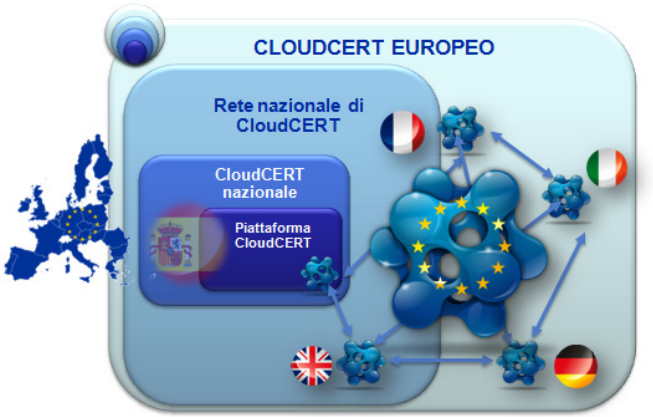
Dopo la realizzazione, la fase successiva del progetto pilota è quella dell'utilizzo della piattaforma. Questa fase può iniziare con l'installazione della piattaforma in un ambiente di produzione reale, allo scopo di creare un CloudCERT nazionale che integri il Centro Nazionale PIC e i principali CERT con abilità inerenti alla PIC e altri possibili attori d'interesse e pertinenti.

FASE 3 – NODI CLOUDCERT (OPPORTUNITÀ)



La prossima fase della roadmap consiste nella riproduzione senza difficoltà in altri stati membri per creare nodi CloudCERT nazionali. Le differenze nei quadri giuridici di ciascun paese possono influire sul corso dello scambio di informazioni. È auspicabile inserire requisiti e condizioni complementari per modificare la piattaforma senza alterare sensibilmente il suo scopo ultimo.

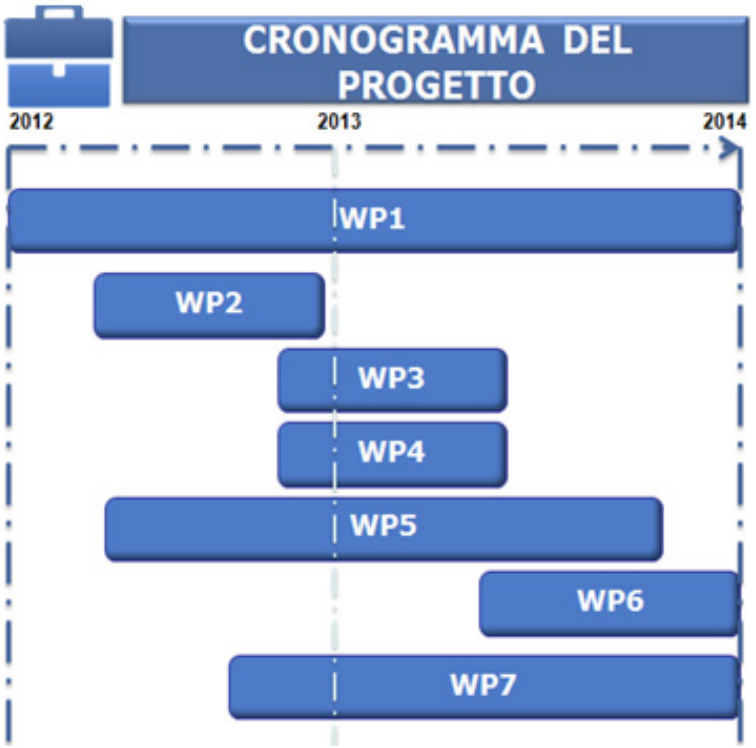
FASE 4 - CLOUDCERT EUROPEO (OPPORTUNITÀ)



Se queste fasi della roadmap hanno esito positivo, la fase finale consisterà nell'interconnessione fra nodi CloudCERT nazionali, che formeranno un CloudCERT europeo composto dalla somma di tutti i membri nazionali, o un CloudCERT paneuropeo che coinvolga i centri Nazionali PIC.

WORK PACKAGE

PANORAMICA DEI WORK PACKAGE



WP1: GESTIONE DI PROGETTO

- Coordinamento dei partner e del loro lavoro.
- Gestione dei rischi.
- Gestione finanziaria.

WP2: MODELLAZIONE E ARCHITETTURA CONCETTUALE

- Progettare l'architettura del sistema in base alla definizione concettuale del sistema della Piattaforma CloudCERT.

WP3: STANDARD D'INFORMAZIONE E DI COMUNICAZIONE

- Definizione del contenuto e del formato delle informazioni da scambiare.
- Definizione del protocollo per scambiare le informazioni.

WP4: DEFINIZIONE DI UN SISTEMA SICURO

- Eseguire un'indagine sulle pratiche di lavoro correnti per una gestione e condivisione sicura di informazioni sensibili e, infine, proporre un elenco di caratteristiche necessarie.

WP5: SVILUPPO DELLA PIATTAFORMA

- Sviluppare un sistema sicuro di condivisione e scambio di informazioni sensibili, con un catalogo e un database di vulnerabilità PIC.

WP6: SPERIMENTAZIONE DELLA PIATTAFORMA PILOTA

- Testare lo strumento della piattaforma in base ai casi d'uso integrativi.

WP7: DIVULGAZIONE DEI RISULTATI DEL PROGETTO

- Divulgazione dei risultati del progetto attraverso pubblicazioni, conferenze, seminari.

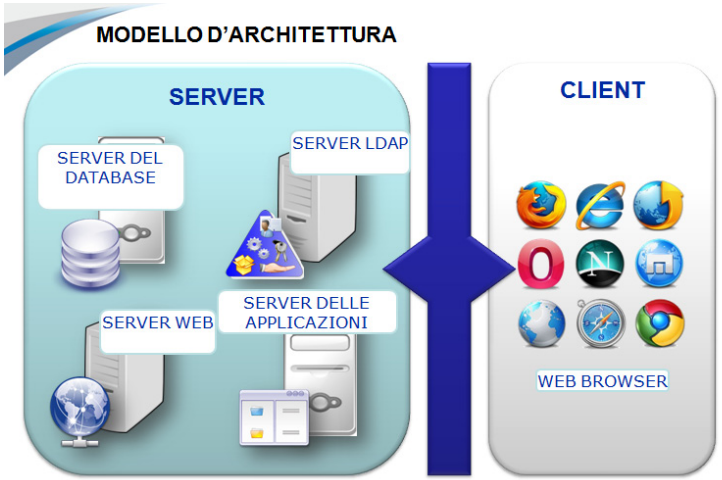
WP1. GESTIONE DI PROGETTO

INTECO, in qualità di coordinatore del Progetto CloudCERT, è il responsabile ultimo del completamento di tutti i work package e il capofila delle attività di gestione del progetto.

WP2. DESIGN DELLA PIATTAFORMA

MODELLO D'ARCHITETTURA

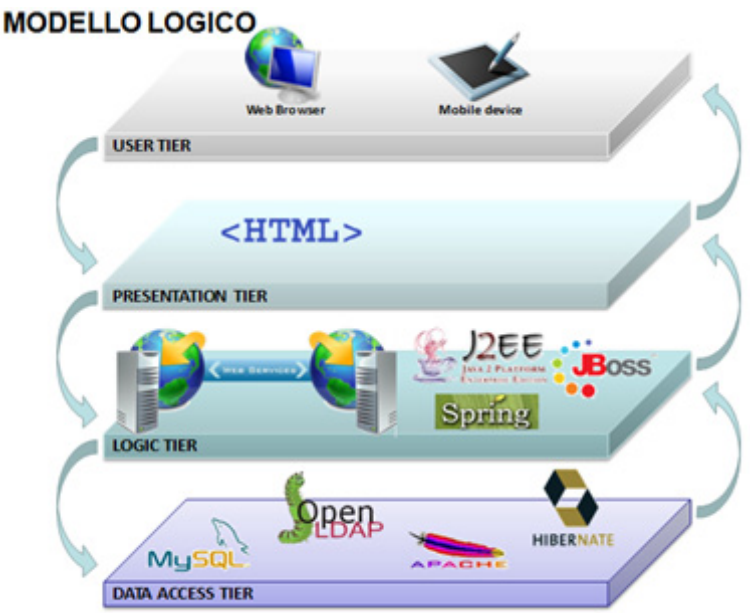
CloudCERT si fonda su un'architettura client / server. Il modello dei diversi componenti della piattaforma CloudCERT si basa sullo standard J2EE.



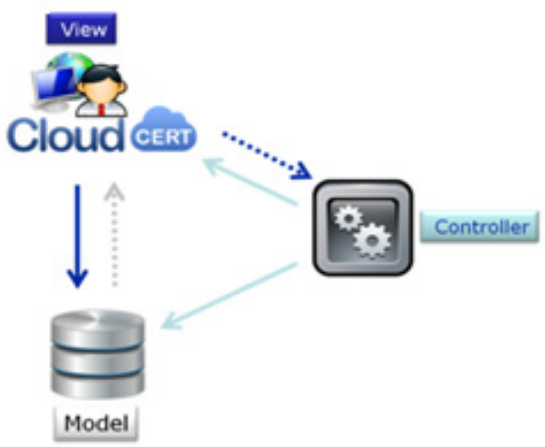
MODELLO LOGICO

I componenti del modello logico della piattaforma sono raggruppati nelle seguenti categorie:

- **Persistenza dei dati.** CloudCERT ha un modello di dati complesso. Per gestire questo modello in modo efficace, sono stati utilizzati alcuni Sistemi.
- **Sicurezza delle Applicazioni.** Tutte le attività correlate alla sicurezza delle applicazioni si basano su informazioni immagazzinate nel LDAP.
- **Gestione del controllo dei flussi di applicazioni**. CloudCERT utilizza il Framework di Struts. Struts è un sistema di supporto per lo sviluppo di applicazioni web su standard MVC sotto la piattaforma J2EE.
- **Servizi Web**. Vengono installati con AXIS CloudCERT. AXIS è un'implementazione SOAP sviluppata da Apache che soddisfa gli standard OASIS e W3C.
- **Livello di presentazione**. Si basa sull'utilizzo dei framework Struts e DWR.



SCHEMA MVC

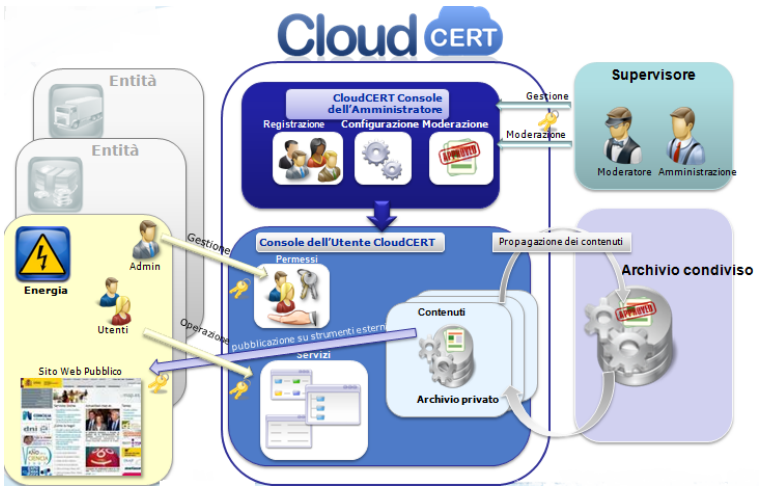


Come la maggior parte delle applicazioni J2EE esistenti, lo schema Modello – Vista – Controllo è stato adottato nella piattaforma CloudCERT.

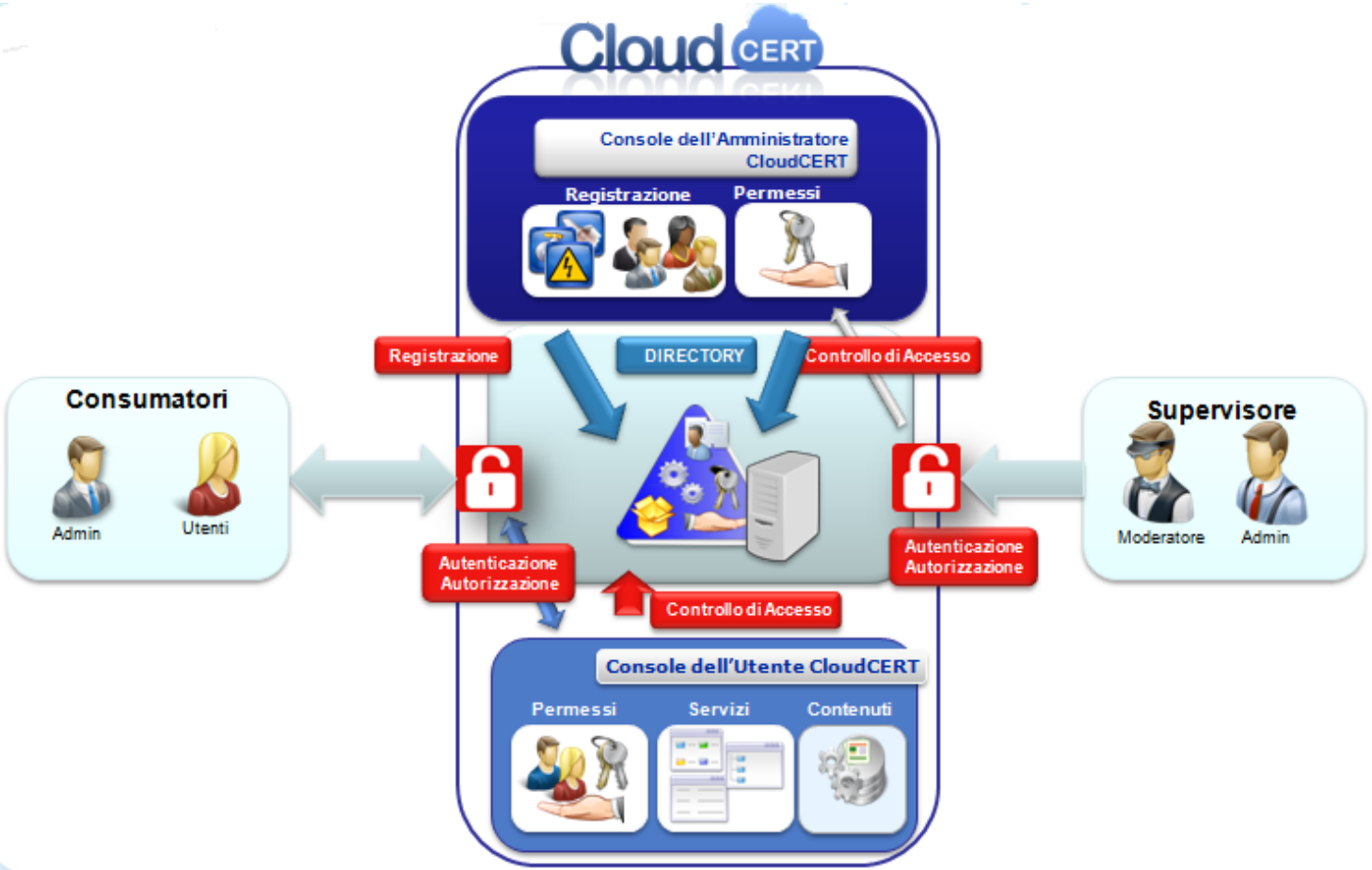
DESIGN FUNZIONALE

Le applicazioni e i moduli che formano la piattaforma CloudCERT includono:

- **Modulo di Autenticazione CloudCERT**: Central Authentication Service (CAS).
- **Modulo di Gestione della Password**: modulo per la gestione delle modifiche alla password e l'attivazione degli account degli utenti.
- **Console dell'Utente CloudCERT**: Console di Gestione delle applicazioni per diverse entità.
- **Console d' Amministrazione CloudCERT**: gestione delle applicazioni per la Piattaforma CloudCERT (servizi, servizi web, entità e contenuti).
- **Servizi WEB CloudCERT.**



SICUREZZA

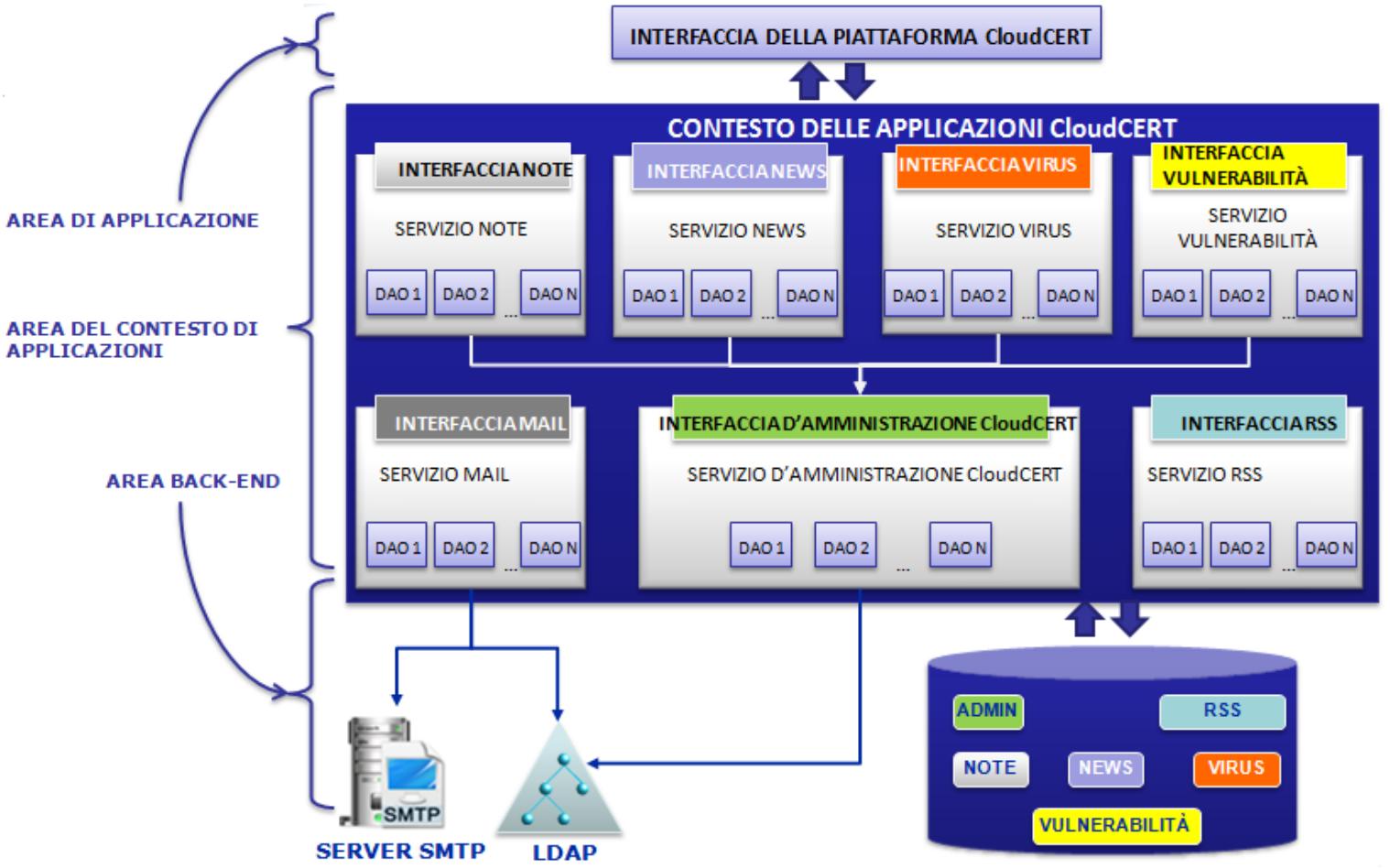


Tutte le questioni riguardanti la sicurezza delle applicazioni si basano sulle informazioni immagazzinate sull'LDAP. I seguenti Framework sono stati utilizzati per gestire la sicurezza di CloudCERT:

- **Spring Security.** Modulo che appartiene al Framework Spring, permette alla logica delle applicazioni di mantenere gratuito il codice di sicurezza, fornendo meccanismi di autenticazione e autorizzazione per le applicazioni J2EE. Inoltre, Spring Security supporta l'autenticazione sul Central Authentication Service (CAS), fornendo un client API per interagire con il server CAS.
- **Spring LDAP** modulo che appartiene allo Spring Framework, fornisce meccanismi di interazione per semplificare operazioni di qualsiasi tipo di server LDAP.

DESIGN GENERALE DEL CONTESTO

Utilizzando la persistenza del Database e dell' LDAP, CloudCERT ha definito un contesto globale accessibile attraverso diverse applicazioni:



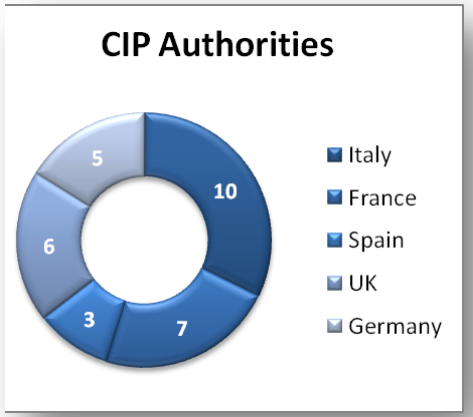
- **Area d'Applicazione.** Spazio che contiene l'intera logica di presentazione e il controllo dei flussi.
- **Contesto dell'area d'applicazione.** Il contesto che definisce i vari servizi offerti da un'interfaccia pubblica alle applicazioni che supportano o altri servizi.
- **Area Back-End.**
  - Database della piattaforma CloudCERT.
  - CloudCERT LDAP.
  - Server SMTP.

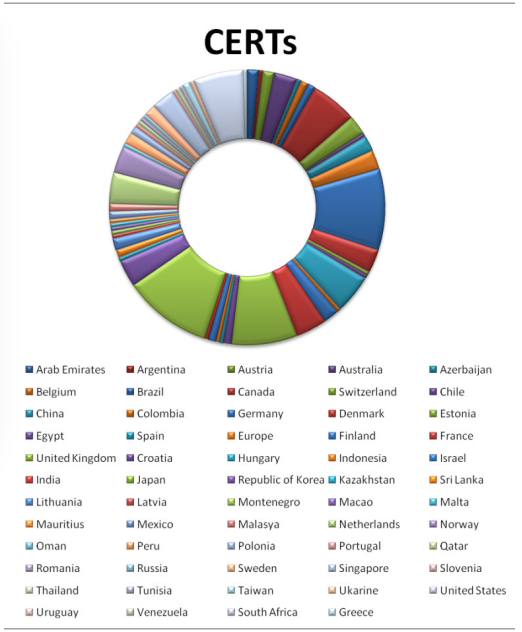
WP3. STANDARD DI INFORMAZIONE E DI COMUNICAZIONE

ONTOLOGIE DEI CONTENUTI DELLE INFORMAZIONI

- **NOTE:** gestire e condividere tutte le informazioni correlate agli eventi istituzionali dei CERT d'interesse generale nella rete della Piattaforma CloudCERT.
- **NEWS:** presentare, gestire e condividere tutte le news pubbliche considerate d'interesse generale.
- **ALLERTA:** presentare, gestire e condividere tutti i casi considerati allerta di particolare interesse.
- **VIRUS:** presentare, gestire e condividere tutti i virus di particolare interesse.
- **VULNERABILITÀ:** gestire e condividere tutte le vulnerabilità di particolare interesse.
- **ELEMENTI RSS:** consultare tutti gli elementi RSS considerati di particolare interesse.

POTENZIALI UTENTI DI CLOUDCERT





PROTOCOLLI PER LO SCAMBIO DI INFORMAZIONI E STANDARD DI DESCRIZIONE DELLE INFORMAZIONI

TECNOLOGIE GENERALI PER LA CONDIVISIONE DI INFORMAZIONI

Fra i vari tipi di **protocolli per la condivisione di informazioni** che sono stati sviluppati nel corso degli anni sono stati selezionati tre protocolli, in parte perché ampiamente utilizzati in diversi tipi di organizzazioni e in parte per la loro flessibilità, che può essere sfruttata positivamente nel contesto di CloudCERT:

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

STANDARD SPECIFICI PER LO SCAMBIO DI INFORMAZIONI PER MOTIVI DI SICUREZZA

Il progetto CloudCERT ha come obbiettivo specifico quello di aiutare gli amministratori delle infrastrutture critiche e delle infrastrutture critiche dell'informazione a difendersi meglio dalle minacce alla sicurezza informatica. I flussi di sicurezza sono (e saranno di certo nel prossimo futuro) una minaccia al funzionamento delle infrastrutture informatiche.

Non appena si scoprono nuovi flussi, informare utenti e amministratori sulle problematiche individuate è fondamentale sia per i venditori di servizi informatici sia per le squadre di sicurezza. Il modo comune per diffondere queste informazioni è attraverso "avvisi di sicurezza", ovvero documenti tecnici che descrivono in modo dettagliato le caratteristiche della problematica, il suo impatto potenziale, e spesso forniscono anche una lista di soluzioni possibili.

Questa sezione è dedicata ai più comuni **formati standard di avviso di sicurezza**:

- 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).

PIANO DI SOLUZIONI ALTERNATIVE

VALUTAZIONE DELLO SCAMBIO DI CONTENUTI

I contenuti che includono informazioni utili sulle allerta di particolare interesse sulla rete di CloudCERT sono adatti ad essere trasferiti con **SOAP** (Simple Object Access Protocol) in **HTTP** (Hypertext Transfer Protocol Secure):

- Allerta.
- Virus.
- Vulnerabilità.

Tuttavia, i seguenti contenuti non sono adatti ad essere condivisi:

- **Note**. Questo contenuto viene utilizzato dagli utenti di CloudCERT per condividere informazioni relative ad eventi istituzionali dei CERT nella piattaforma di rete.
- **News**. Questo contenuto viene utilizzato dagli utenti di CloudCERT per condividere link a URL collegati alle news pubbliche dei CERT prive di particolare interesse al di fuori della piattaforma di rete.
- **Elementi RSS**. Questo contenuto è utilizzato dagli utenti CloudCERT per condividere gli elementi RSS di diversi feed pubblici.

INDICATORI

È importante gestire con attenzione la condivisione di qualsiasi contenuto con altre organizzazioni. A questo scopo, è stato necessario integrare un modulo dashboard nella piattaforma CloudCERT che permettesse all'amministratore di tenere sotto controllo una serie di indicatori legati a quest'attività. Gli indicatori individuati per il monitoraggio erano:

- Numero di elementi prodotti in uno specifico periodo di tempo.
- Numero di elementi letti in uno specifico periodo di tempo.
- La Top N dei contenuti più letti.
- La Top N delle organizzazioni più attive nella produzione.
- La Top N delle organizzazioni più attive nella lettura.
- La Top N delle organizzazioni più attive nell'importazione di contenuti (da archivi condivisi a archivi privati).
- Distribuzione mensile delle giornate di maggiore attività in termini di produzione/consumo di contenuti.

WP4. DEFINIZIONE DI UN SISTEMA SICURO

PRATICHE DI LAVORO PER UNA GESTIONE E CONDIVISIONE SICURA DELLE INFORMAZIONI SENSIBILI

La piattaforma CloudCERT ha l'obiettivo di facilitare lo scambio di **informazioni sensibili** sulla PIC fra diversi tipi di attori garantendone la sicurezza. Pertanto, la prima attività del work package è un sondaggio volto a studiare le pratiche di lavoro che consentono una gestione e condivisione sicura delle informazioni sensibili.

SICUREZZA DELLE INFORMAZIONI

In questo capitolo si descrive l'ambito della sicurezza delle informazioni e le principali problematiche ad essa associate, con particolare attenzione ai Sistemi di Informazione.

- **Riservatezza**: l'eventuale divulgazione inappropriata delle informazioni deve essere individuata ed evitata.
- **Integrità**: le informazioni non devono essere modificate da soggetti non autorizzati.
- **Disponibilità**: le informazioni devono essere a disposizione dei soggetti autorizzati ove richiesto.

CONDIVISIONE DELLE INFORMAZIONI PER LA PIC

Questo capitolo ripercorre quanto è stato fatto per permettere una condivisione efficace delle informazioni nel contesto della PIC dai governi di due fra i più importanti paesi del mondo: gli Stati Uniti e il Regno Unito.

PROTEZIONE DELLE INFRASTRUTTURE CRITICHE

Sono stati presi come esempio due paesi e i loro piani di PIC sono stati descritti e analizzati dettagliatamente: le politiche elaborate dagli Stati Uniti e la situazione italiana:

- Strategia Nazionale per la Sicurezza Interna.
- Quadro Strategico Nazionale Italiano per la sicurezza cibernetica.

REQUISITI DI SICUREZZA DI CLOUDCERT

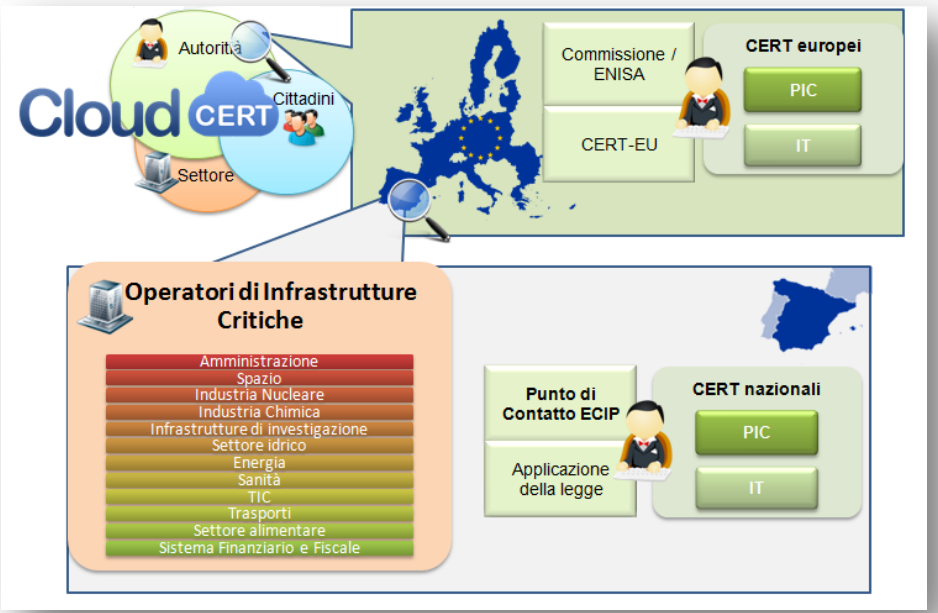
I principali obiettivi di questo prodotto finale sono:

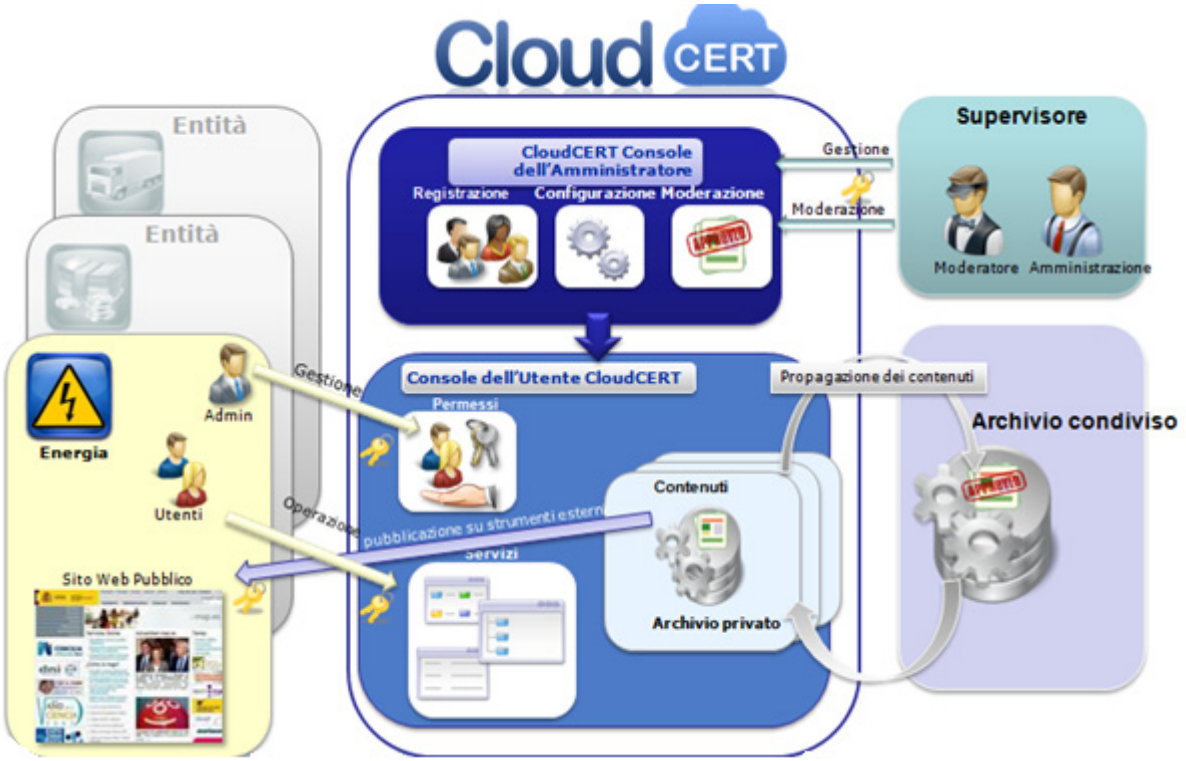
- Individuare le principali fonti scientifiche nell'ambito della PIC.
- Individuare metodi e procedure ipotetiche per estendere e rafforzare i processi di collaborazione nel sistema.
- Individuare metodi e procedure ipotetiche per estendere e rafforzare la capacità di coordinamento fra gli attori del sistema durante il ciclo di vita dell'IC.

Lo scopo ultimo di tutti gli obiettivi è aggiornare il modello operativo di governance per attribuire ruoli, responsabilità e obiettivi agli attori del sistema.

Gli attori CloudCERT sono suddivisi in tre categorie principali:

- **Autorità** (settore pubblico): autorità competenti nella sicurezza delle informazioni e protezione delle infrastrutture critiche, a livello sia legale che operativo, inclusi politici, legislatori e forze dell'ordine.
- **Industria** (settore privato): operatori delle infrastrutture critiche, inclusi i loro principali fornitori (fabbricanti di prodotti e sviluppatori di servizi).
- **Cittadini** (pubblico target): utenti di servizi forniti da infrastrutture critiche.





Questi attori interagiscono con la piattaforma CloudCERT in base ad un modello di governance che si articola nel modo seguente:

- Diverse **entità** possono avere accesso alla Piattaforma: CERT, forze dell'ordine, e operatori di infrastrutture critiche. Ogni entità ha il proprio spazio in cui distribuire contenuti e può importare contenuti dall'archivio condiviso. I contenuti possono essere esportati automaticamente in strumenti esterni come il sito web interno dell'entità.
- Un'organizzazione di **supervisione**:
  - **Gestisce** la piattaforma registrando le organizzazioni e il loro utente amministratore, e configurando e gestendo i servizi disponibili. Il supervisore configura le autorizzazioni delle varie entità ad accedere ai contenuti e servizi stabiliti per contratto.
  - Fornisce la **moderazione**. Tutti i contenuti devono essere soggetti a moderazione e far parte dell'**archivio condiviso**. La moderazione riguarda anche le pubblicazioni in strumenti come forum, wiki, ecc.
- Ogni entità ha un **utente amministratore** che può creare utenti e concedere autorizzazioni alla sua Entità. I contenuti dell'archivio privato dell'entità possono essere pubblicati in un archivio condiviso con l'approvazione del supervisore.
- Gli **utenti** possono interagire con i contenuti e i servizi della piattaforma.

WP5. SVILUPPO DELLA PIATTAFORMA

È la fase di implementazione del progetto pilota. In quest'ottica, vengono svolte le seguenti attività:

REQUISITI E ANALISI

La descrizione dei requisiti del software ha la funzione di:

- Individuare requisiti e funzionalità della piattaforma CloudCERT ponendo domande agli utenti finali.
- Registrare i requisiti del sistema di sicurezza e dello scambio di informazioni sensibili.
- Definire e classificare in base alle priorità i requisiti della piattaforma CloudCERT.

SVILUPPO

In base alla metodologia agile **scrum**, la fase di sviluppo include:

- L'implementazione dei requisiti definiti nella fase precedente, per creare un modello funzionale pilota.
- La creazione della documentazione dell'utente e dell'amministrazione del modello pilota sviluppato.

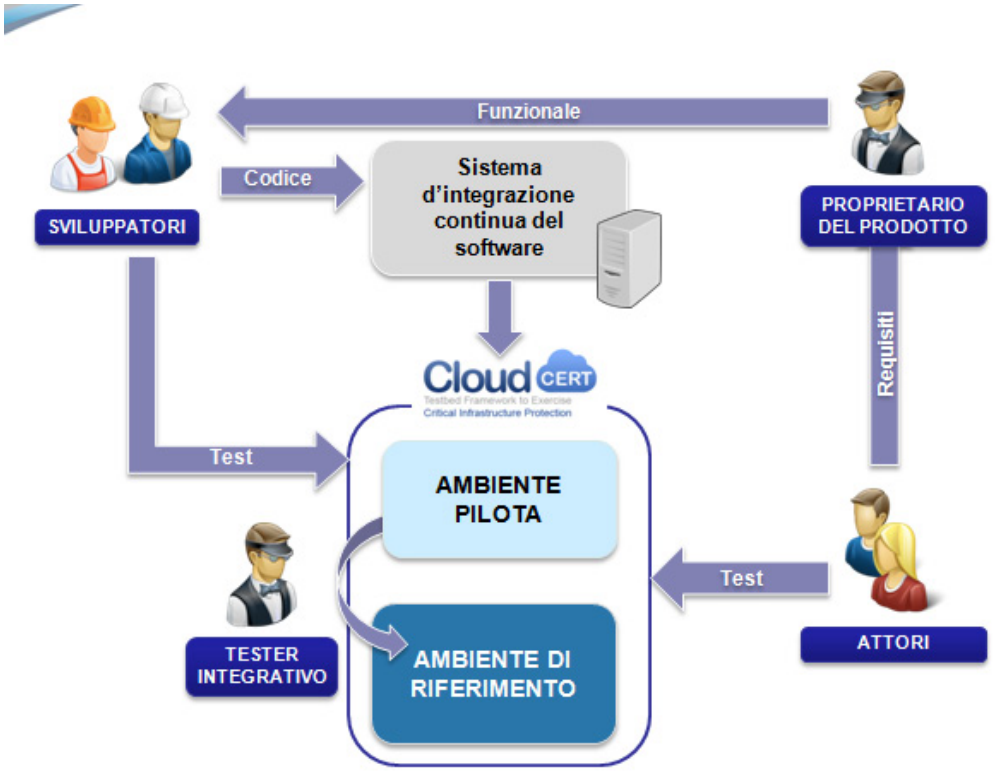
INSTALLAZIONE E CONFIGURAZIONE DELLA PIATTAFORMA

Durante questa fase, vengono predisposti gli ambienti di sviluppo e testing, e vengono prodotti manuali di installazione e configurazione.

AMBIENTI

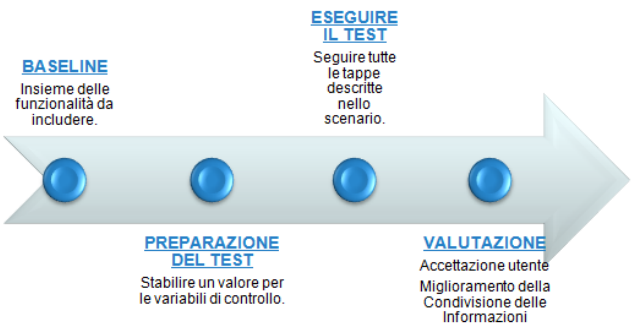
L' **ambiente pilota** viene utilizzato per caricare e testare nuovi sviluppi, e per verificarli dopo ogni sprint.

Una volta conclusa la fase di testing e verificato ogni aspetto, il nuovo prodotto viene inserito nell'**ambiente di riferimento**, che contiene una versione più stabile della Piattaforma CloudCERT.



WP6. SPERIMENTAZIONE PILOTA

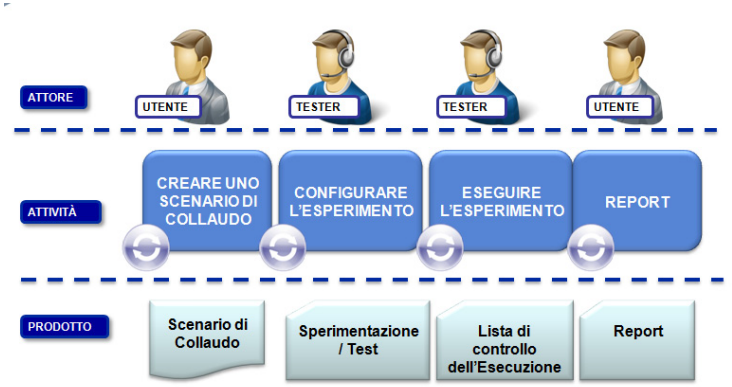
Le attività del WP6 si concentrano sulla sperimentazione e valutazione basata sui casi d'uso integrativi, sulla Piattaforma Pilota sviluppata e installata nei precedenti WP. Le attività includono il testing funzionale e l'accettazione del prodotto, ma anche esercizi di simulazione sullo scambio di informazioni fra utenti della piattaforma per sperimentare e dare dimostrazione dei casi simulati, dello scambio di informazioni sulla scoperta delle vulnerabilità, le allerta e gli avvisi di sicurezza e la denuncia degli incidenti di sicurezza.

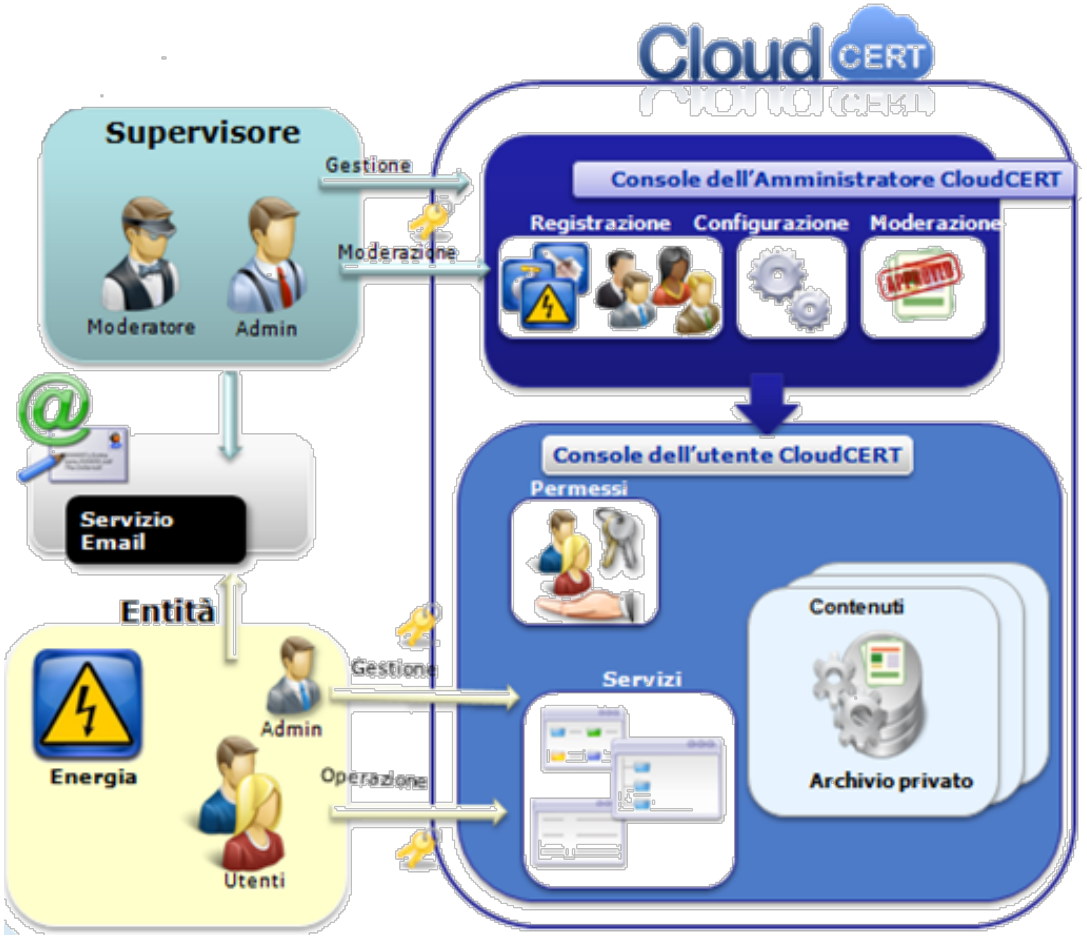


L'obiettivo della valutazione e della sperimentazione è utilizzare la sperimentazione attraverso scenari d'uso come base per valutare il contributo della soluzione della piattaforma CloudCERT per migliorare la collaborazione e cooperazione fra gli attori della PIC nella condivisione di informazioni sulla sicurezza informatica, e testare così la funzionalità e i flussi di lavoro disponibili perché la comunicazione possa avere luogo.

L'obiettivo della valutazione, che si basa sui risultati della sperimentazione, è:

- testare CloudCERT (se i processi di condivisione delle informazioni sono supportati correttamente);
- verificare in che modo CloudCERT risponde alle sfide e alle necessità del settore in termini di collaborazione e cooperazione;
- e valutare i potenziali miglioramenti nella PIC resi possibili da CloudCERT.





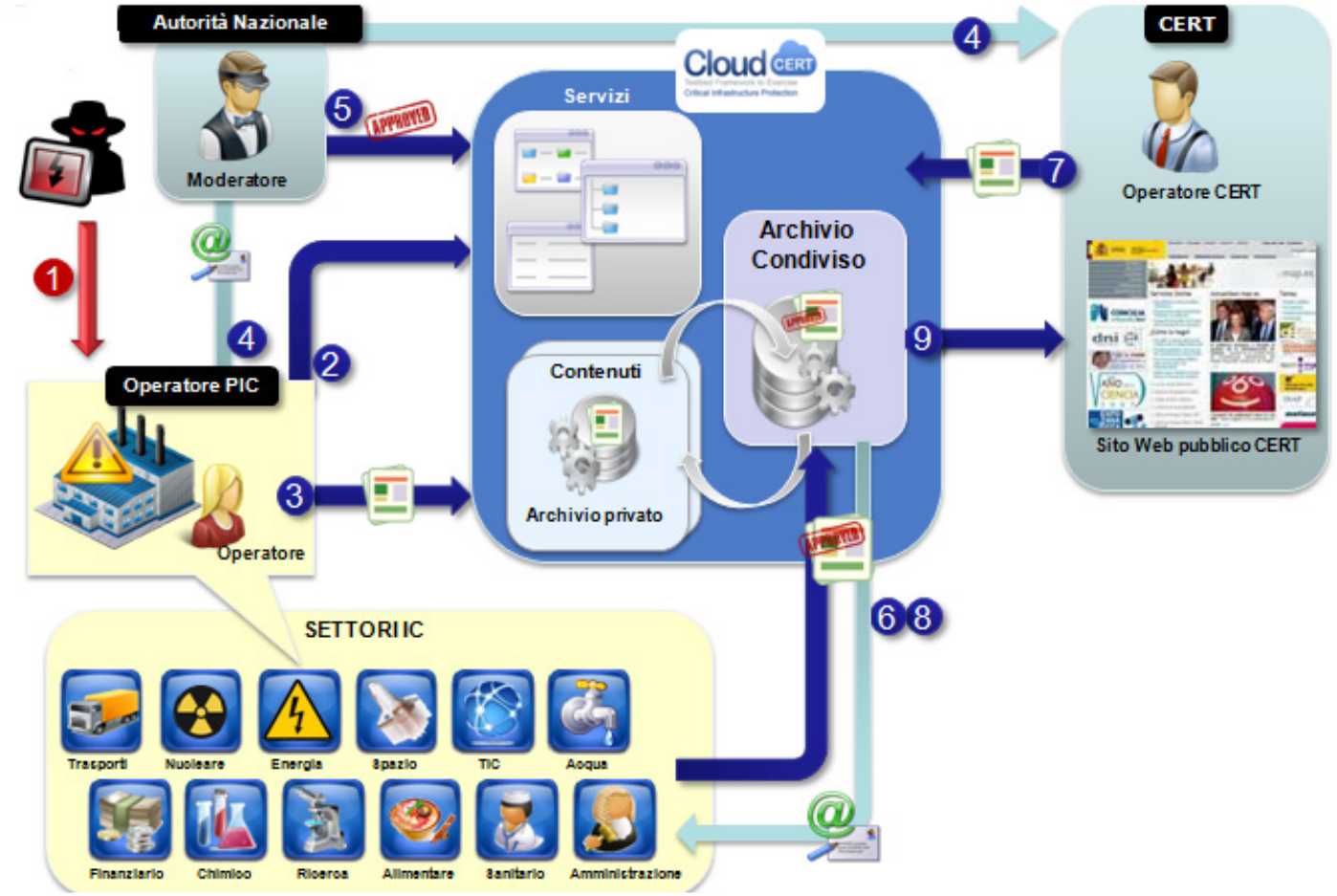
STRUMENTI PER LA SPERIMENTAZIONE

- **Console d'Amministrazione CloudCERT.** Permette di gestire interamente le funzionalità della piattaforma CloudCERT.
- **Console dell'Utente CloudCERT**. Facilita la creazione, l'implementazione e il funzionamento di nuove entità per rispondere agli incidenti di sicurezza.
- **Client E-mail.**

ATTORI

- Utente – Operatore IC.
- Amministratore – Operatore IC.
- Moderatore. – CERT / Autorità
- Amministratore.- Autorità

ESEMPIO DI SCENARIO DI CASO D'USO

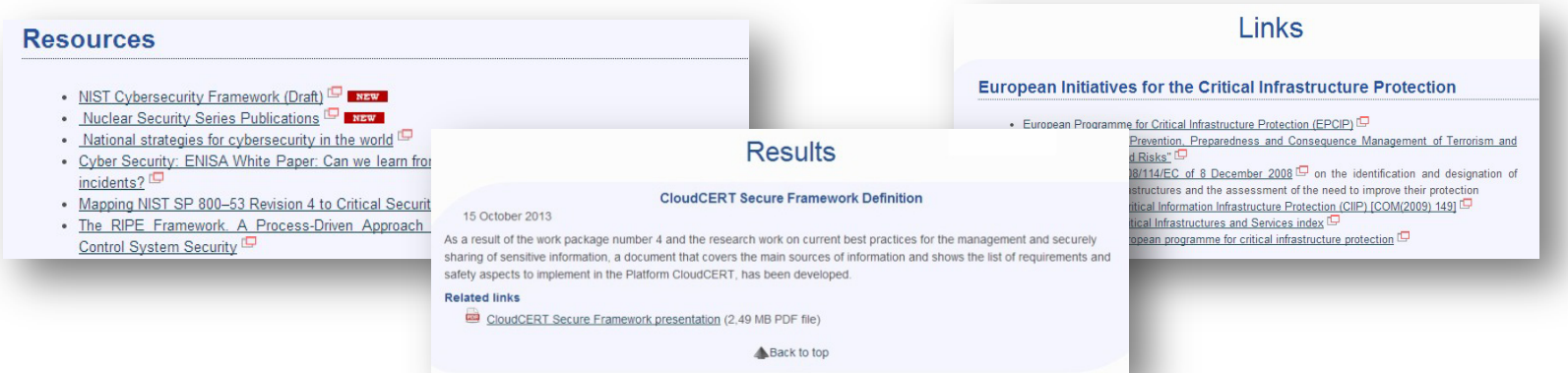


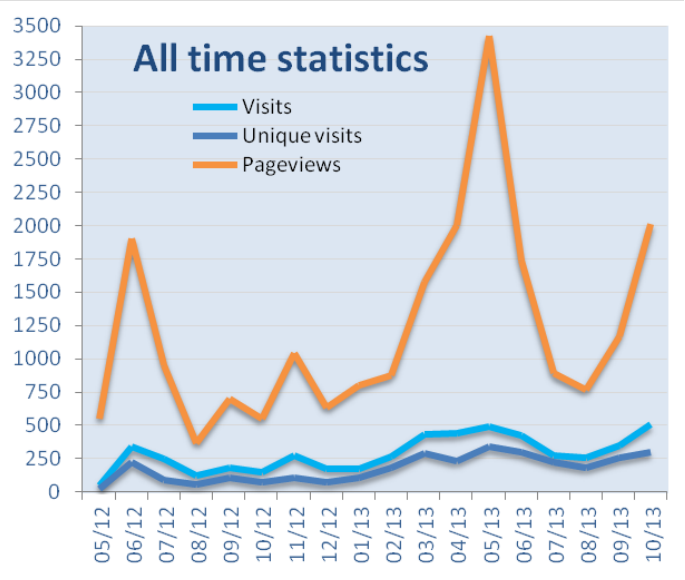
1. L'operatore **individua una vulnerabilità** su un prodotto e un'intrusione sulla rete interna.
2. Cerca informazioni e legge la Procedura per la gestione degli Incidenti su **wikiCIP**.
3. Crea un'allerta e dei post sul **Forum**.
4. Procedura ufficiale di **denuncia** dell'incidente.
5. CNPIC **convalida** l'allerta.
6. **and 8. L'allerta** è visibile su CloudCERT e via e-mail attraverso il bollettino di informazione.
7. CERT **risolve l'allerta** e chiude il post sul forum con una soluzione temporanea.
9. L'allerta viene pubblicata su un **sito web esterno**.

WP7. DIVULGAZIONE DEI RISULTATI DEL PROGETTO

Gli indicatori più rilevanti del sito web del progetto CloudCERT **http://cloudcert.european-project.eu/** :

- Più di **200** news pubblicate.
- Più di **5.000** visite (ricevute).
- Più di **40** risorse condivise.
- Più di **22.000** visualizzazioni della pagina (ricevute).





WIKIPEDIA

- Inglese: http://en.wikipedia.org/wiki/CloudCERT
- Spagnolo: http://es.wikipedia.org/wiki/CloudCERT
- Italiano: http://it.wikipedia.org/wiki/CloudCERT

EVENTI

2012

- CRITIS12 Conferenza sulla Sicurezza delle Infrastrutture Critiche dell'Informazione. http://critis12.hig.no/

2013

- Young Researchers Innovation Week
- 8° Workshop CERT ENISA.
- Protezione delle Infrastrutture Critiche – Telecomunicazioni.

CloudCERT

Testbed Framework to Exercise Critical Infrastructure Protection

Cloud CERT
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

18 de septiembre de 2012 | 18:29 CET

PROYECTOS

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

La Comisión Europea seleccionó el proyecto Cloud CERT del Instituto Nacional de Tecnologías de la Comunicación (INTECO), dirigido a desarrollar una plataforma para ejercicios específicos de cooperación en la seguridad de las infraestructuras críticas en la Unión Europea. El Instituto pondrá en valor la experiencia de INTECO CERT en esta materia, los estándares de comunicación segura, y otros desarrollos que ha llevado a cabo relacionados con la seguridad en las infraestructuras críticas. INTECO será el líder del proyecto, que tendrá una duración de dos años y un presupuesto estimado de 454.962,73 euros. Del consorcio también forman parte CNPIC (ES), Indra (ES), Zanasi Alessandro Srl. (IT), Europe for Bussiness Ltd (UK), ICSA (IT), y como asociado Theodore Puskas Foundation (HU).

Raúl Riesco / Ignacio Cano

CONFERENZA FINALE

Conferenza finale CloudCERT per divulgare i risultati del progetto europeo fra il pubblico target.

- **Data:** 22 Novembre 2013.
- **Luogo:**
  - Segreteria di stato per le telecomunicazioni e la società dell'informazione (SETSI). Madrid (Spagna)
- **Pubblico target:**
  - Attori del progetto CloudCERT.
  - Operatori delle infrastrutture Critiche Spagnole inclusi i principali fornitori e venditori.
  - Altri CERT europei e forze dell'ordine coinvolte nella PIC.
- **Accesso:**
  - Accesso libero su invito e video trasmissione in streaming. http://www.cloudcert.webcastlive.es.


Spain, 22 November 2013

CloudCERT

Testbed Framework to Exercise Critical Infrastructure Protection

Publication date: 28.10.13
Subject: CloudCERT final conference

Final Conference of CloudCERT European Project to Present Results Achieved

The CloudCERT European Project, which is co-financed by the European Union (E.U.) and whose project consortium is co-ordinated by INTECO, is holding its **Final Conference on 22 November at the Spanish Secretariat of State for Telecommunications and the Information Society (SETSI) in Madrid.** The conference will present the results obtained during the execution of the project (2012 to 2013), demonstrating the CloudCERT platform for sharing cyber-security information that it has produced, as well as the various other deliverables generated by the project.

The CloudCERT Project provides a test-bed environment for the exchange of information on Critical Infrastructure Protection (CIP) and its security aspects, enabling co-operation and co-ordination of the agents involved so as to manage cyber-risk-critical assets effectively.

The EU has supported this project financially through the specific programme entitled "Prevention, Preparedness and Consequence Management of Terrorism and Other Security-Related Risks", falling within the "Security and Safeguarding Liberties" framework programme.

The project consortium is made up of the National Institute for Communication Technologies (INTECO), a company dependent upon the Ministry of Industry, Energy and Tourism (MINETUR) through the Secretariat of State for Telecommunications and the Information Society (SETSI) (Spain) **as project co-ordinator**, together with the National Centre for Critical Infrastructure Protection (CNPIC) of the Ministry of the Interior (Spain), Indra (Spain), ZANASI and Partners (Italy) , Europe for Business Ltd. (United Kingdom) and the ICSA Foundation (Italy).


Conference

CloudCERT

Testbed Framework to Exercise
Critical Infrastructure Protection

Agenda

09h00 Registration

09h30 Welcome reception

10h00 CloudCERT project:
- Background of the project.
- Project objectives and motivation.
- Project results and main deliverables.

11h15 Coffee Break

11h45 CloudCERT Pilot:
- Exchanging critical infrastructure information security.
- Demo.

13h00 Next steps for the project and Closing remarks

22/11/2013


CloudCERT

CloudCERT project
Juan Diez González - INTECO

Cloud CERT European Project

English Presentación Vistas Descargas

Madrid, 22 noviembre 2013 | © Barcode 2013

SOLUZIONE TECNOLOGICA

PIATTAFORMA COLLABORATIVA

CLOUDCERT PUÒ ESSERE INTERESSANTE PER VOI?

- Se la vostra organizzazione è un **CERT o un Operatore IC**, potete utilizzare questa piattaforma per gestire gli incidenti sulle Infrastrutture Critiche e condividere informazioni sulla sicurezza informatica.
- Se l'ambito di attività della vostra organizzazione come **CERT o Autorità** include **operatori di infrastrutture critiche**, potete ottenere una piattaforma personalizzata per fornire servizi e strumenti per le vostre attività di protezione delle infrastrutture critiche (forum, wiki, ecc).
- Se la vostra organizzazione deve interagire con **Autorità Nazionali per la Protezione delle Infrastrutture Critiche**, e in base alle sue competenze a livello nazionale, potete assegnare i ruoli più adeguati all'interno della piattaforma: coordinamento, supervisione, partecipazione, ecc.

CONTENUTI

La piattaforma CloudCERT vi permette di creare e diffondere contenuti sulla sicurezza, come:

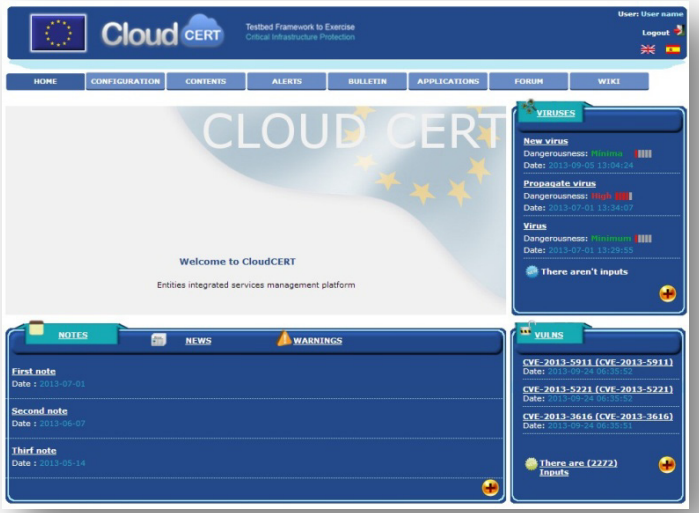
- Note.
- News.
- Allerta.
- Virus.
- Vulnerabilità.
- Elementi RSS.

SERVIZI E STRUMENTI

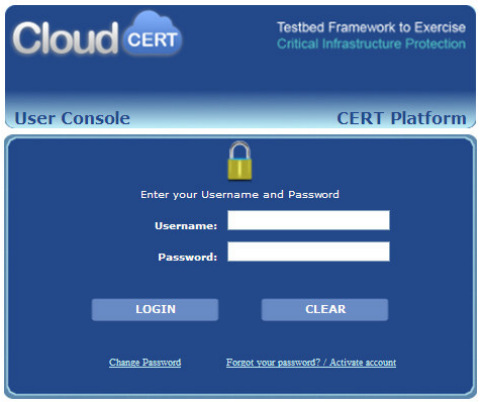
La piattaforma CloudCERT permette agli utenti di condividere informazioni per evitare incidenti di sicurezza attraverso i suoi servizi:

- Forum.
- WikiCIP.
- Bollettino di informazione.

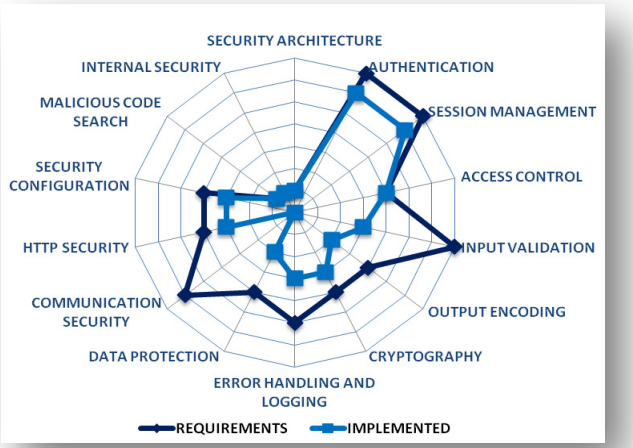
SCHEDA DEL PRODOTTO



- **Piattaforma Collaborativa** per gestire un archivio condiviso di informazioni sulla sicurezza informatica collaborando in modo efficace.

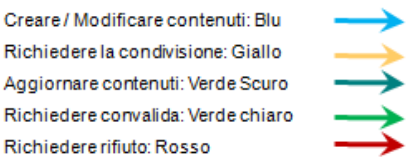


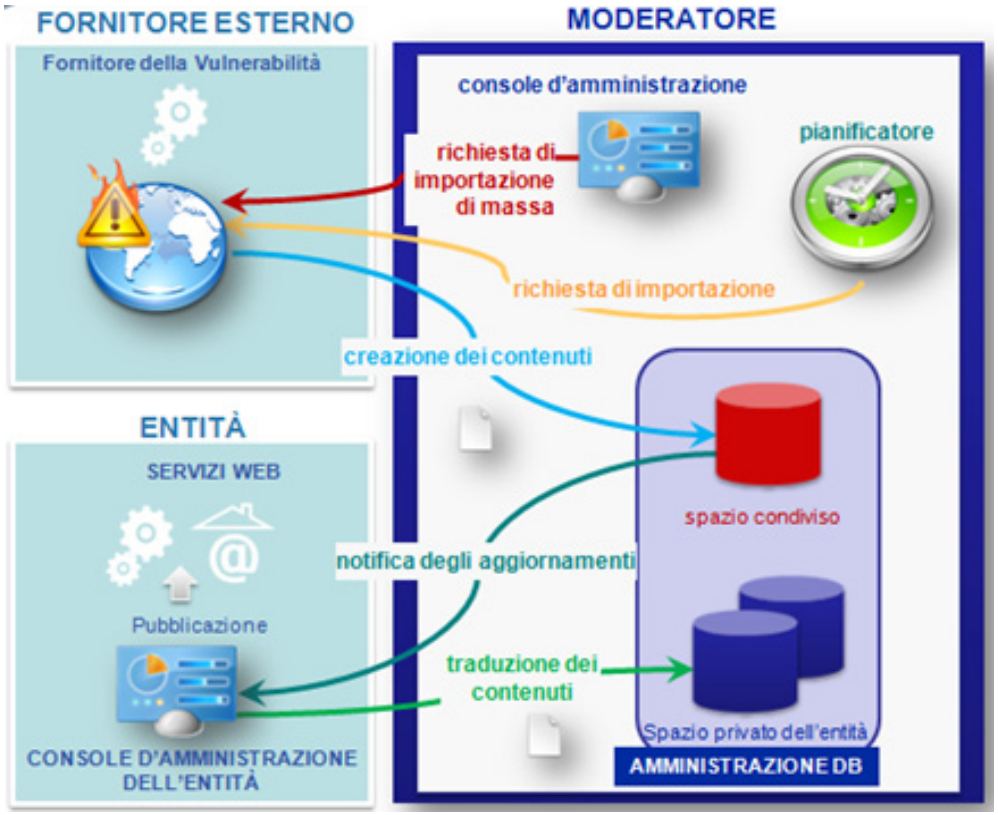
- Paradigma **Cloud** basato su **archivi condivisi** e privati.
- **Applicazione multi-lingue** e interfaccia di traduzione dei contenuti.
- **Servizi personalizzati** (stabiliti per contratto).
- Piattaforma **scalabile** che permette di inserire nuovi contenuti, servizi, strumenti e flussi di lavoro
- **Ambiente sicuro**:
  - Meccanismo di autenticazione basato su username e password: Central Authentication Service (CAS).
  - Autorizzazione basata su permessi e ruoli.
  - Gestione sicura delle sessioni.
  - Garanzia di riservatezza e protezione dei dati.



CICLO DI VITA DEI CONTENUTI

- CloudCERT permette la creazione e l'**aggiornamento** dei contenuti (informazioni strutturate) in maniera collaborativa.
- Ogni entità tiene i contenuti nel suo **spazio privato** e può richiedere di condividerli.
- Un moderatore revisiona i contenuti da pubblicare nell'**archivio condiviso**.
- Le entità possono **estrarre** i loro contenuti e pubblicarli in strumenti esterni (ad esempio intranet).



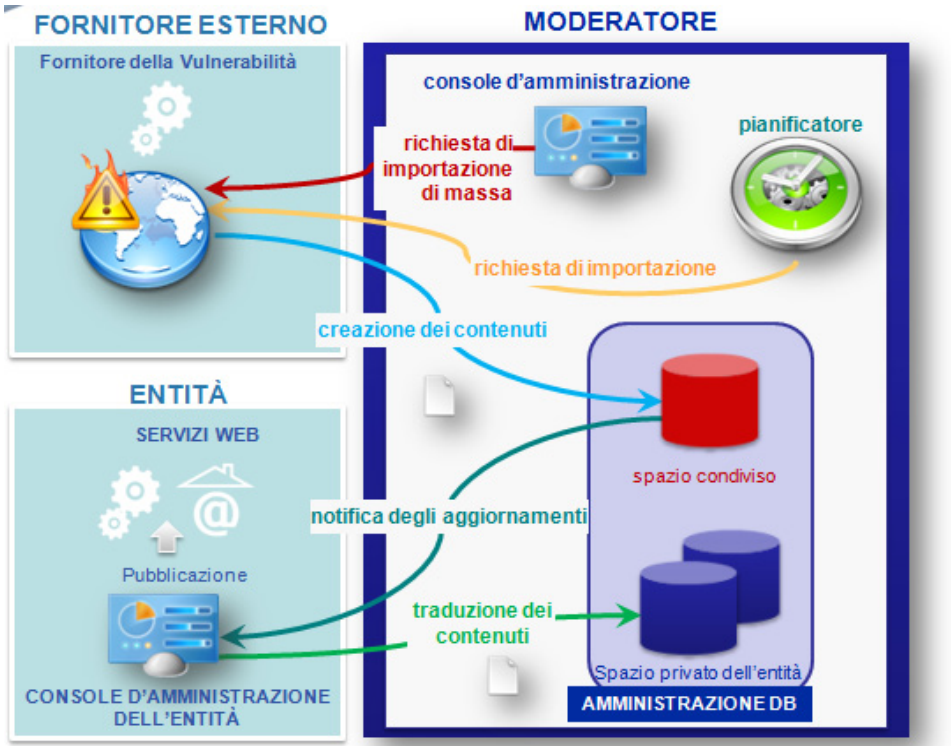


I contenuti possono trovarsi nei seguenti stati durante il loro ciclo di vita:

- Creati.
- Modificati.
- Condivisi.
- Aggiornati.
- Convalidati.
- Respinti.

CICLO DI VITA DELLE VULNERABILITÀ

- Le vulnerabilità sono un tipo specifico di contenuto fornito attraverso **risorse esterne** (come i NIST).
- Una procedura programmata **importa** automaticamente le vulnerabilità nel sistema.
- Il moderatore può anche **richiedere un'importazione di massa** (per un periodo di tempo) nel sistema.
- Le entità possono **tradurre le vulnerabilità** nel loro spazio privato.



Archiviazione delle vulnerabilità: Blu
Richiesta di importazione incrementale: Giallo
Notifica degli aggiornamenti: Verde scuro
Traduzione delle vulnerabilità: Verde chiaro
Richiesta di importazione di massa: Rosso

Dunque, una vulnerabilità può trovarsi in uno dei seguenti stati durante il suo ciclo di vita:

- Importata.
- Notificata (aggiornamento).
- Tradotta.

WIKICIP

Un wiki è un sistema flessibile che permette all'amministratore di definire gerarchie di pagine. WikiCIP permette di gestire **contenuti non strutturati** in maniera collaborativa, mettendo a disposizione i seguenti elementi strutturali:

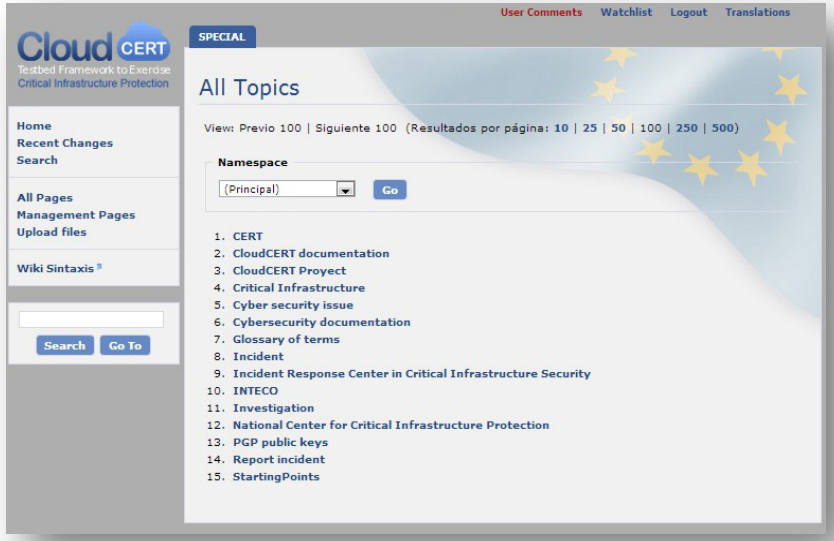
- **Indice** – Pagina dell'indice contenente link a diverse pagine wiki con argomento simile.
- **Pagina** – Pagine individuali su un argomento specifico.

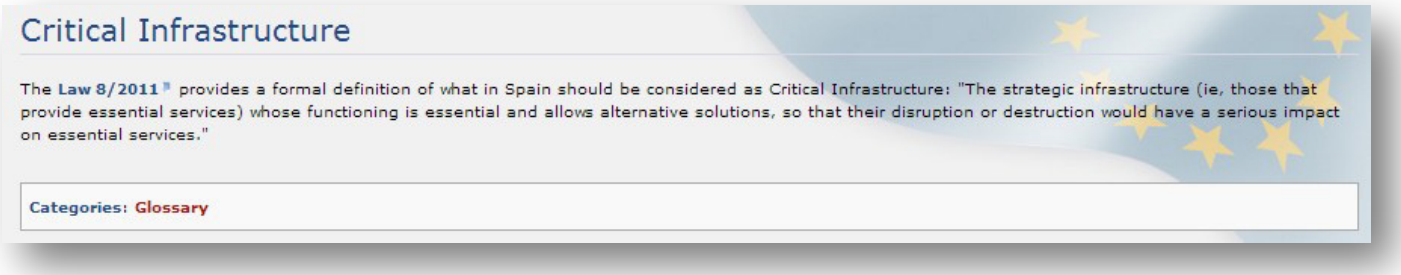
WikiCIP ha la seguente struttura di argomenti:

- **Documentazione CloudCERT**:
  - Presentazione generale del progetto e delle risorse principali.
    - Manuale dell'utente.
    - Manuale dell'amministratore.
    - Manuale dello sviluppatore.

- **Documentazione sulla sicurezza informatica**:
  - Procedura operativa sugli incidenti di sicurezza informatica.
  - Quadro giuridico.
  - Link interessanti sulla PIC.

- **Glossario.** Principali termini relativi alla Protezione delle Infrastrutture Critiche.

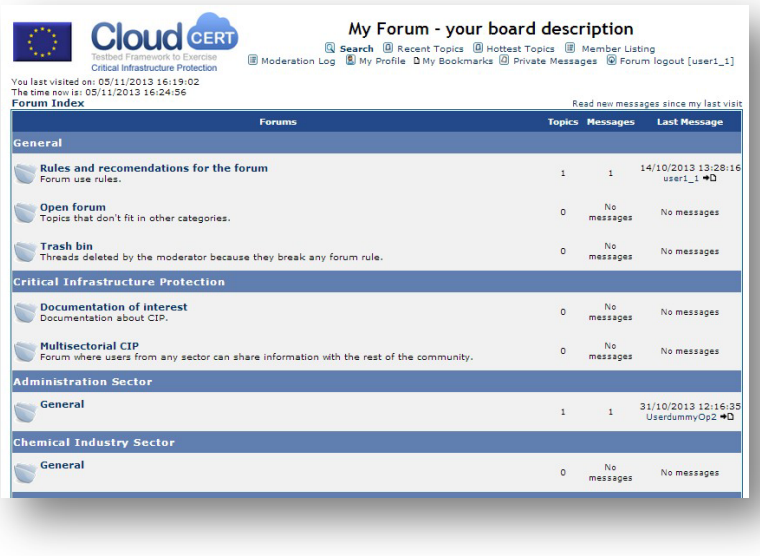




FORUM

Il forum permette lo scambio di informazioni non strutturate con i seguenti elementi di classificazione:

- **Categoria**. È l'elemento più importante della gerarchia e, di solito, viene utilizzato per raggruppare diversi forum correlati. È un gruppo logico, e ogni forum all'interno di una categoria ha il proprio ciclo di vita.
  - **Forum**. Un forum è un insieme di discussioni sullo stesso argomento.
    - **Discussione** o **Topic**. È la discussione stessa, i messaggi degli utenti su un argomento specifico.



Il Forum CloudCERT comprende le seguenti categorie:

- **Generale**. Forum sulle informazioni generali.
- **Protezione delle Infrastrutture Critiche**. Gli utenti possono discutere o condividere informazioni generali sulla protezione delle infrastrutture critiche con il resto della comunità.
- Ogni operatore di infrastrutture critiche ha un forum riservato al suo **settore** (secondo la classificazione legale nazionale spagnola sulla PIC) in cui gli utenti possono condividere informazioni con altri attori rilevanti del settore.
  - Amministrazione.
  - Spazio.
  - Industria nucleare.
  - Industria chimica.
  - Strutture investigative.
  - Risorse idriche.
  - Energia.
  - Sanità.
  - Tecnologie dell'Informazione e della Comunicazione (TIC).
  - Trasporti.
  - Settore alimentare.
  - Sistema finanziario e fiscale.

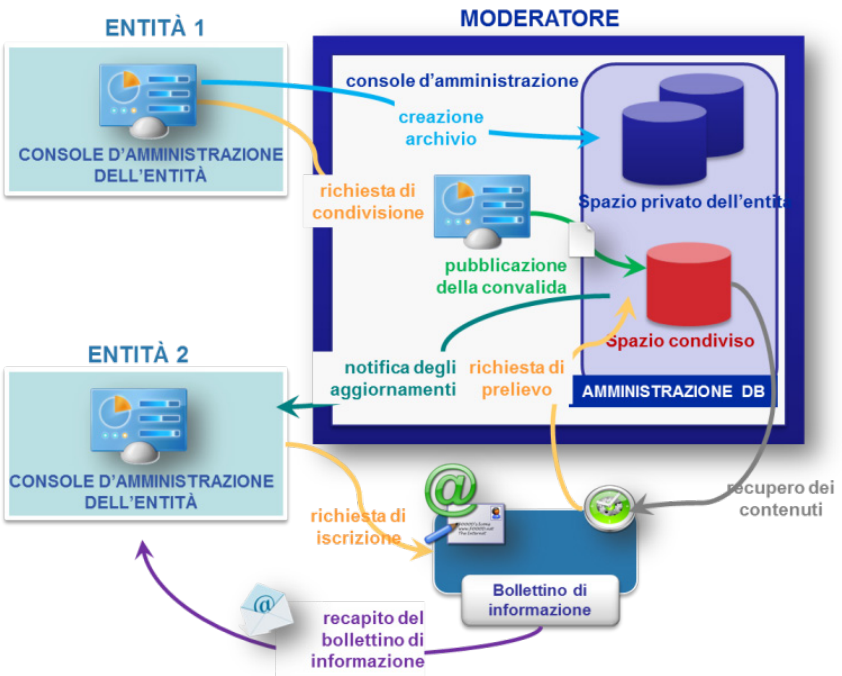
BOLLETTINO DI INFORMAZIONE

Il bollettino di informazione è un servizio esterno che comunica con la Piattaforma CloudCERT per **ricevere le iscrizioni degli utenti** e **accedere ai contenuti immagazzinati** nei database CloudCERT per creare i bollettini. Il servizio è responsabile della creazione e formattazione dei bollettini, e del recapito degli stessi agli utenti finali in base alle loro preferenze.

Ogni entità registrata CloudCERT può iscrivere gli utenti (già registrati o esterni) a diversi bollettini sulla sicurezza, per ricevere periodicamente informazioni direttamente nella posta in arrivo dell'e-mail.

L'iscrizione può essere effettuata dall'amministratore dell'entità o dall'utente finale.

- Il bollettino di informazione permette agli utenti di tenersi informati sugli aggiornamenti dei contenuti attraverso notifiche via e-mail.
- Per selezionare il tipo di bollettino e di contenuti, è necessario seguire un processo d'iscrizione.
- Il servizio raccoglie contenuti, crea bollettini personalizzati e li recapita ad ogni utente finale.



Creazione dei contenuti: Blu

Richieste: Giallo

Notifica di aggiornamento: Verde scuro

Richiesta di convalida: Verde chiaro

Richiesta di importazione di massa: Rosso

Recupero dei contenuti per la creazione del bollettino di informazione: Grigio

Recapito del bollettino di informazione: Viola

Cloud CERT

Testbed Framework to Exercise
Critical Infrastructure Protection

CloudCERT - Sistema di valutazione per esercitare la protezione delle infrastrutture critiche.

HOME/2010/CIPS/AG/20.
Con il supporto finanziario del Programma Prevenzione, Preparazione e Gestione delle Conseguenze in materia di Terrorismo e di altri Rischi correlati alla Sicurezza. Commissione Europea – Direzione Generale Giustizia, Libertà e Sicurezza.