Cloud CERT

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

CONTATO

http://cloudcert.european-project.eu

info@cloudcert.european-project.eu

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

RESULTADOS DO CLOUDCERT - QUADRO DE BANCO DE ENSAIO PARA EXERCÍCIO DE PROTEÇÃO DE INFRAESTRUTURA CRÍTICA

Editado:
Instituto Nacional de Tecnologías de la Comunicación SA - INTECO
Avenida José Aguado, 41-24005 León
987 877 189
www.inteco.es

Versão eletrônica disponível em:

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

ÍNDICE

1. JUSTIFICATIVA e MOTIVAÇÃO 4
   1.1. Resumo do programa 5
   1.2. Motivação 5
   1.3. Escopo 5

2. DESCRIÇÃO DO PROJETO 7
   2.1. Participantes 8
   2.2. Objetivos 9
   2.3. Benefícios 9
   2.4. Grupo Alvo 9
   2.5. Dimensão Europeia do projeto e roteiro 10

3. PACOTES DE TRABALHO 8
   3.1. Visão geral dos Pacotes de Trabalho 14
   3.2. PT1. Gerenciamento de Projeto 15
   3.3. PT2. Design da Plataforma 16
   3.4. PT3. Normas de Informação e Comunicação 20
   3.5. PT4. Definição de quadro seguro 23
   3.6. PT 5. Desenvolvimento da plataforma 26
   3.7. PT 6. Experimentação piloto 28
   3.8. PT 7. Divulgação dos resultados do Projeto 31

4. SOLUÇÃO TECNOLÓGICA 34
   4.1. Plataforma colaborativa 35
   4.2. Ciclo de vida do conteúdo 37
   4.3. Vulnerabilidades do ciclo de vida 38
   4.4. WikiCIP 39
   4.5. Fórum 40
   4.6. Boletins de Serviço 41

JUSTIFICATIVA E MOTIVAÇÃO

RESUMO DO PROGRAMA

A segurança e economia da União Europeia, bem como o bem-estar dos seus cidadãos, dependem de certas infraestruturas e os serviços que prestam. A destruição ou rompimento da infraestrutura de fornecimento de serviços essenciais pode implicar a perda de vidas, a perda da propriedade, um colapso da confiança pública e moral na UE.

2004 A fim de neutralizar essas vulnerabilidades, o Conselho Europeu solicitou, em 2004, o desenvolvimento de um Programa Europeu de Proteção das Infraestruturas Críticas (PEPIC). Desde então, um trabalho de preparação abrangente foi realizado, que incluiu a organização de seminários relevantes, a publicação de um Livro Verde, as discussões com os agentes públicos e privados e ao financiamento de um projeto piloto.

2006 Com isso em mente, em 12 de dezembro de 2006, a Comissão adotou a comunicação sobre um PEPIC, que definiu um quadro horizontal global para atividades críticas de proteção da infraestrutura no nível da UE. O Programa da UE propôs em "Prevenção, preparação e gestão das consequências em matéria de terrorismo e outros riscos de segurança conexos" foi adotada em 12 de Fevereiro de 2007.

2008 A Diretiva de 2008/114/CE do Conselho, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção criado um procedimento para identificação e designação das infraestruturas críticas europeias (ICE). Ao mesmo tempo, fornece uma abordagem comum para avaliar estas infraestruturas, com vista a melhorá-los para proteger melhor as necessidades dos cidadãos.

2009 Finalmente, em 30 de março de 2009, a Comissão adotou a comunicação sobre Proteção de Informações Infraestruturas Críticas (PICI) [COM (2009) 149], que dá detalhes sobre os principais desafios que as infraestruturas de informação críticas e propõe um plano de ação, destinado a aumentar a sua proteção.

HOME/2010/CIPS/AG/20

O Programa da UE sobre "Prevenção, preparação e gestão das consequências do terrorismo e outros riscos de segurança conexos" visa encorajar o intercâmbio de *know-how* e de boas práticas entre os vários agentes responsáveis pela gestão de crises e de organizar exercícios conjuntos para melhorar a coordenação entre os departamentos competentes.
A Comissão Europeia elabora programas de trabalho anuais para cobrir as prioridades dentro de cada ano. Estes programas incluem chamadas de propostas para determinar subvenções de ação para ser conferido a projetos transnacionais e /ou nacionais que deverão contribuir para a realização do objetivo geral e também dos específicos do programa. Como resultado deste convite à apresentação de propostas para 2010, este projeto "CloudCERT" foi selecionado como um dos projetos premiados.

MOTIVAÇÃO

Como se afirma no PEPIC Open em uma nova janela, os *stakeholders* devem compartilhar informações sobre a Proteção das Infraestruturas Críticas (PIC), em particular sobre as medidas referentes à segurança da infraestrutura crítica e sistemas protegidos, estudos de interdependência e PIC relacionado com as vulnerabilidades, ameaças e avaliações de risco.
Ao mesmo tempo, deve haver garantia de que as informações de natureza particular, confidencial ou pessoal compartilhada não serão divulgadas publicamente, que qualquer pessoal que lida com informações sigilosas terão um nível adequado de habilitação de segurança por seu Estado-Membro.

Para resolver esse necessidade real, o projeto CloudCERT visa proporcionar esta informação segura compartilhando o quadro de banco de ensaio, a fim de exercer a coordenação unificada usando mesmos padrões de protocolo de comunicação para melhorar a visibilidade de avisos de ameaça comum, vulnerabilidades, lembretes e alertas específicos para o CIP.
A fim de atingir esse objetivo, uma obra importante deve ser feita a partir de um modelo conceitual baseado na comunicação CSIRT e arquitetura; definição de informação segura partilha; normas de informação e definição de protocolo, design da plataforma banco de ensaio e, finalmente, implantar um piloto para verificar a realidade com base em cenários de usuários.

O escopo deste projeto está restrito à criação da plataforma piloto CloudCERT para trocar informações CIP. Deste modo, apenas cobre a primeira fase do roteiro à exposição em longo prazo.
A plataforma final é um piloto operacional, com uma comunidade de usuários e informações úteis o suficiente para testar a sua funcionalidade e realizar exercícios de simulação para a troca de informações PIC.

A plataforma permite a troca de CIP medidas operacionais, metodologias, experiências e know-how entre os usuários que agem como um repositório de informações, incluindo pelo menos os seguintes tipos de informação:

- Vulnerabilidades.
- Notas, Lembretes e Alertas.
- Avisos de ameaça.
- Notícias.
- CIP melhores práticas.
- CIP lições aprendidas.

A plataforma CloudCERT é tecnicamente baseado em uma aplicação web com gerenciamento de usuários, incluindo autenticação forte e troca segura de informações de acordo com normas interoperáveis.

DESCRIÇÃO DO PROJETO

PARTICIPANTES

COORDENADOR

- INTECO - Instituto Nacional de Tecnologias da Comunicação.

CO-BENEFICIÁRIOS

- CNPIC - Centro Nacional de Proteção das Infraestruturas Críticas.
- Europe for business.
- Fondazione Inteligência Cultura e Análise Estratégica (ICSA).
- Indra Systems, Inc.
- INTECO - Instituto Nacional de Tecnologias da Comunicação.
- Zanasi & Partners.

PARCEIROS USUÁRIOS

- INTECO - Instituto Nacional de Tecnologias da Comunicação.
- CNPIC - Centro Nacional de Proteção das Infraestruturas Críticas.

OBJETIVOS

- Para fornecer uma abordagem do **quadro do banco de ensaio** para integrar mecanismos de coordenação de parcerias e esforços dos *stakeholders* para trocar efetivamente informações relacionadas a CIP e os aspectos de segurança.
- Para **proteger a infraestrutura da** UE melhorar a compreensão das relações entre os seus elementos e a ligação entre gestão de riscos e proteção de infraestrutura.
- Para fornecer a capacidade necessária para **eliminar possíveis vulnerabilidades** na infraestrutura crítica, compartilhando informações de vulnerabilidade.
- Para **gerenciar a segurança** como um todo através de um processo unificado de troca de informações para determinar o risco e decidir e implementar ações para reduzir o risco a um nível definido e aceitável, a um custo aceitável.
- Para **obter o valor** derivado de sua troca de informações através da aplicação de exercícios, medida na eficácia da prevenção, deter e responder a ataques cibernéticos em sistemas de controle dentro da infraestrutura crítica.
- Um **relato comum** de **troca de informações** sobre as seis fases do ciclo de vida do CIP, a fim de criar uma solução abrangente.

BENEFÍCIOS

O impacto esperado a **curto prazo** é de fornecer corpos CIP com uma plataforma de banco de ensaio projetado para apoiar o intercâmbio dos Estados-Membros CIP com troca de informação, coordenação e supervisão.

Em **médio prazo**, CloudCERT irá melhorar a cooperação através da implementação da plataforma em um ambiente de produção real que vai contribuir para a minimização dos obstáculos de cooperação para operadores de CIP e autoridades de proteção em diferentes países da Europa.

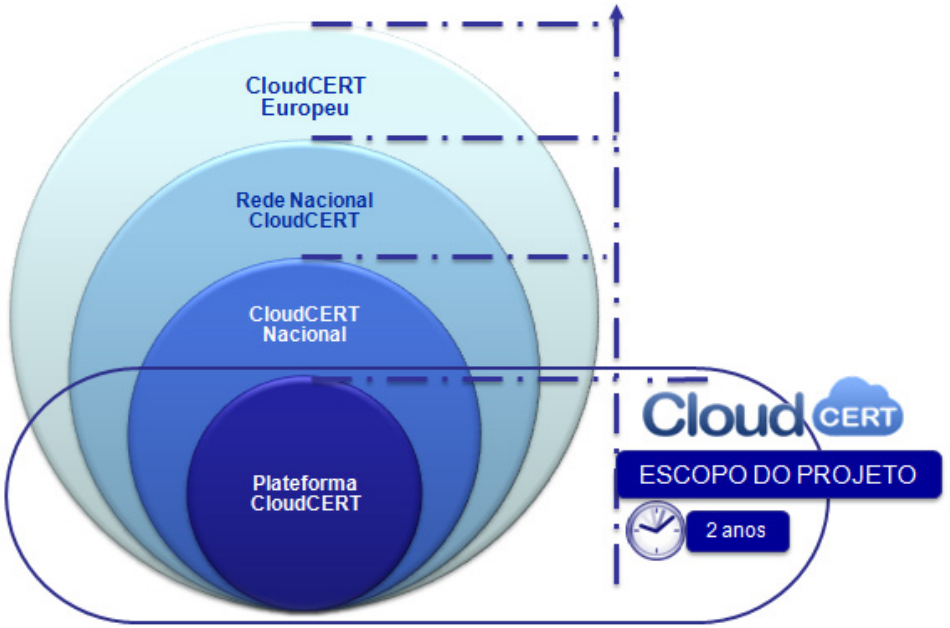
Em **longo prazo**, espera-se contribuir para o estabelecimento de um ambiente de segurança europeia de defesa interna para a proteção dos CIs europeus..

GRUPOS ALVO

Os principais grupos-alvo e beneficiários deste projeto são:

- Os Estados-Membros através das autoridades de Proteção das Infraestruturas Críticas.
- CERT ou CSIRT competentes no CIP.
- Operadores ou proprietários de infraestrutura crítica (CI).

PROJETO DIMENSÃO EUROPÉIA E ROTEIRO



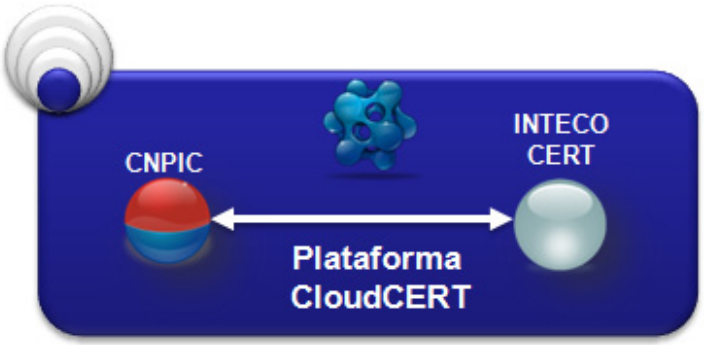
O CloudCERT é um **projeto transnacional**, que envolve parceiros em pelo menos dois Estados-Membros.

A abordagem do projeto em longo prazo segue um roteiro com as seguintes etapas:

- Plataforma CloudCERT .
- CloudCERT Nacional.
- Rede CloudCERTs Nacional.
- CloudCERT Européia.

Para construir uma rede de colaboração pan-europeia, propomos uma metodologia baseada em sucessivas abordagens suplementares, gerando produtos em fases que vão melhorar em cada interação. Durante o período de duração do projeto (2 anos), apenas a **plataforma piloto** é criada com o objetivo em mente de construir um CloudCERT Nacional.

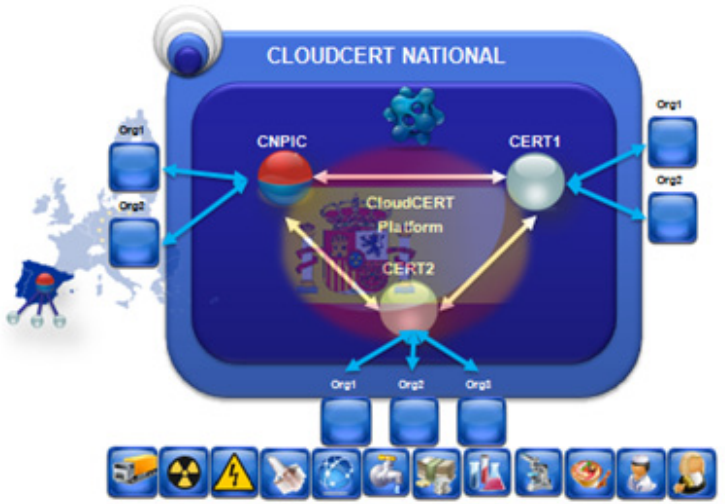
FASE 1 - CLOUDCERT PILOTO (ATUALMENTE CONCEDIDOS PELA UE)



Nesta primeira fase de roteiro, o objetivo é a criação da plataforma piloto para adicionar como usuários da plataforma, atores CIP dentro de um país.

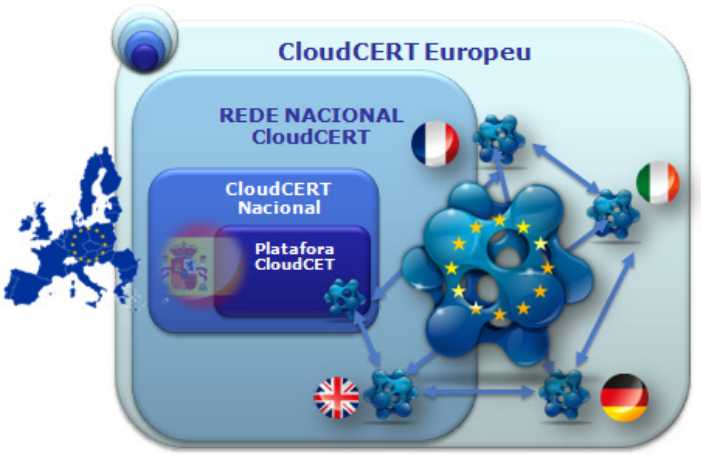
Devido às limitações do projeto, os usuários desta plataforma serão os participantes "CERT" no projeto (INTECO-CERT), bem como os participantes do Centro Nacional de PIC (CNPIC).

FASE 2 - CLOUDCERT NACIONAL (OPORTUNIDADE)



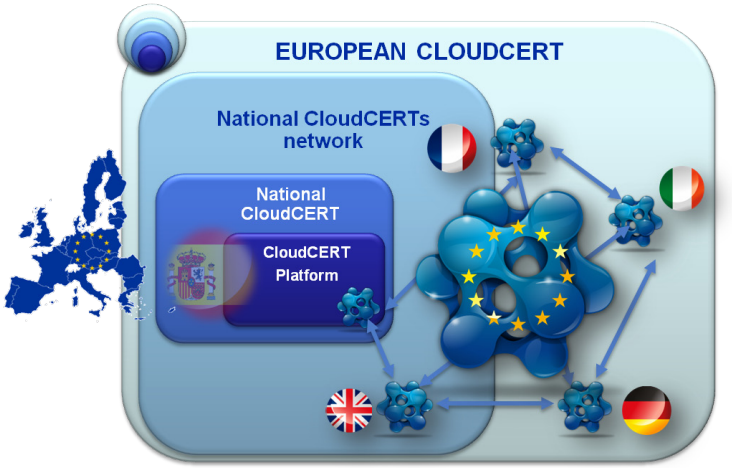
Uma vez liberado o piloto, conduziria à fase de exploração da plataforma. Esta etapa pode começar nesta fase, assim com a implantação da plataforma em um ambiente de produção real, com a fim de estabelecer um CloudCERT Nacional, que integra o Centro Nacional CIP, bem como grandes CERT com recursos da CIP e outros atores possíveis de interesse e relevância .

FASE 3 – NÓS DO CLOUDCERTS (OPORTUNIDADE)



A próxima etapa roteiro poderia ser a replicação, sem dificuldades, em outros países membros para criar nós nacionais CloudCERT. Diferenças no marco regulatório de cada país pode condicionar a troca de informações a se estabelecer. Seria desejável adicionar qualificação ou condições menores para modificar a plataforma, mas não alterar drasticamente ou alterar o seu objetivo principal.

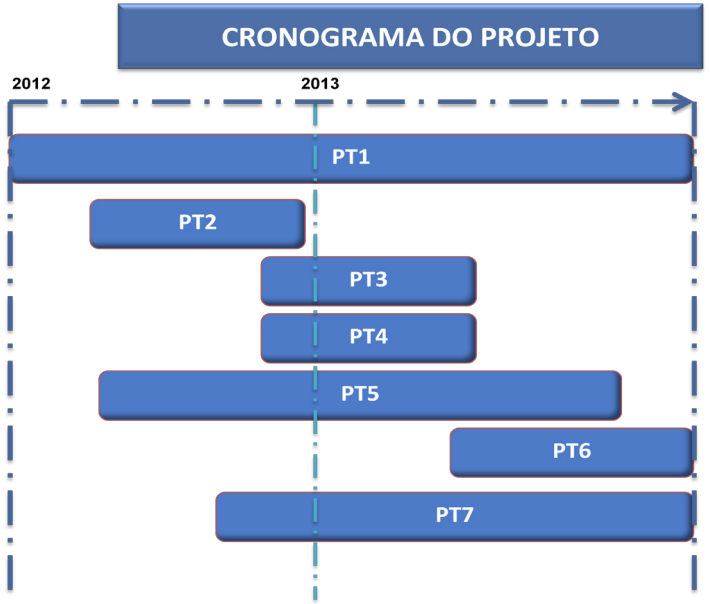
FASE 4 - CLOUDCERT EUROPÉIA (OPORTUNIDADE)



Se estes passos do roteiro são bem sucedidos, uma fase final poderia representar a interligação dos nós CloudCERT Nacional, formando um CloudCERT Européia com a soma de todos os membros nacionais, ou CloudCERT Pan-Européia envolvendo os Centros Nacionais de CIP.

PLANO DE TRABALHO

VISÃO GERAL DO PLANO DE TRABALHO



PT1: GERENCIAMENTO DE PROJETOS

- Coordenação de parceiros e do seu trabalho.
- A gestão de riscos.
- Gestão financeira.

PT2: DESIGN DA PLATAFORMA

- Projetar a arquitetura do sistema com base na definição conceitual do sistema de Plataforma CloudCERT.

PT3: NORMAS DE INFORMAÇÃO E COMUNICAÇÃO

- Definição do conteúdo e formato da informação a ser trocada.
- Definição do protocolo para troca de informações.

PT4: DEFINIÇÃO DE QUADRO SEGURO

- Para investigar práticas de trabalho atuais para gerenciamento seguro e compartilhamento de informações críticas e, finalmente, propõe uma lista de recursos necessários.

PT5: DESENVOLVIMENTO DE PLATAFORMA

- Para desenvolver um compartilhamento seguro de troca de informações sensíveis, catálogo e banco de dados de vulnerabilidades da CIP.

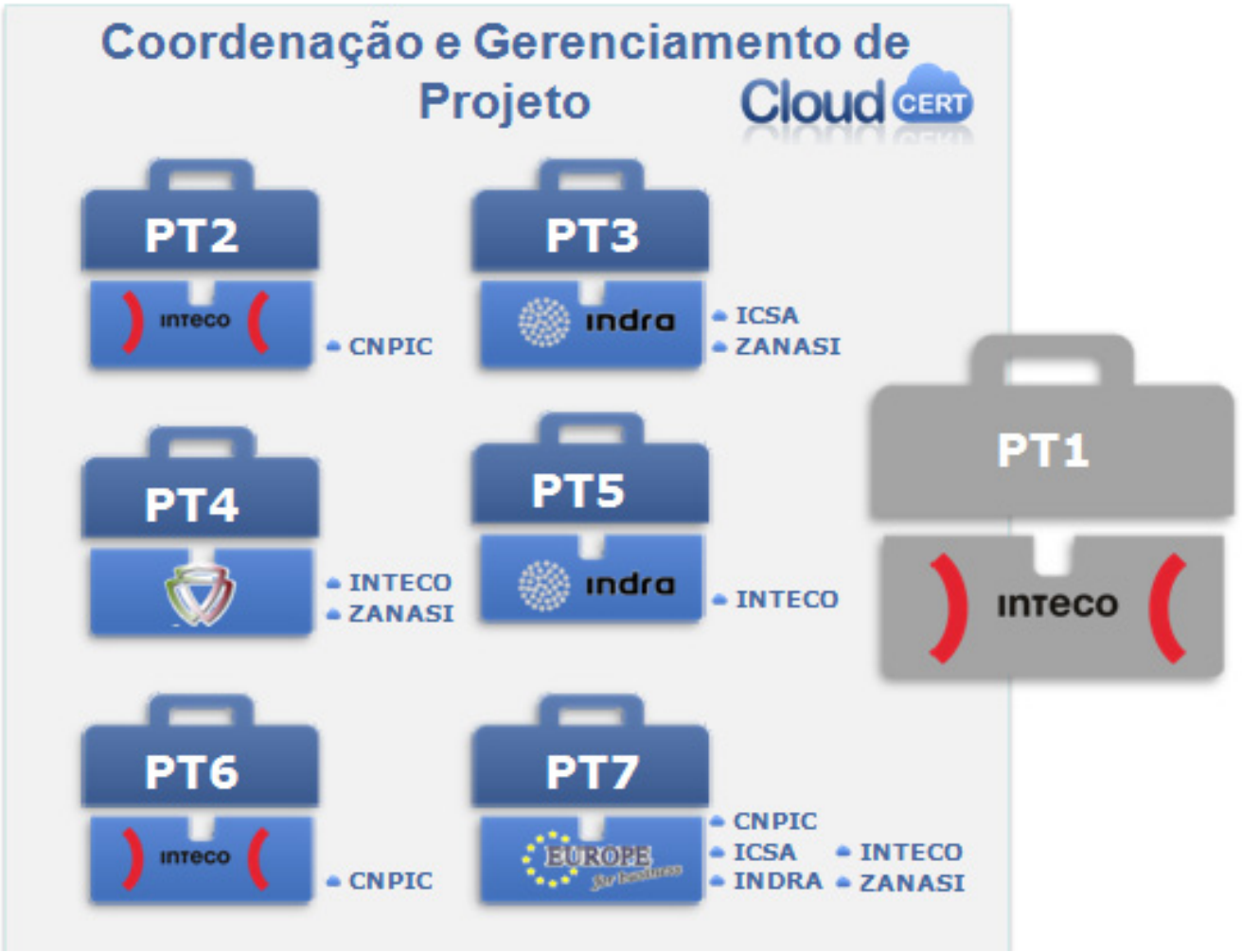
PT6: EXPERIMENTAÇÃO PILOTO

- Para testar ferramenta plataforma com base nos casos de usuários de integração.

PT7: DIVULGAÇÃO DOS RESULTADOS DO PROJETO

- Divulgação de resultados do projeto através de publicações, conferências, seminários.

PT1. GERENCIAMENTO DE PROJETO

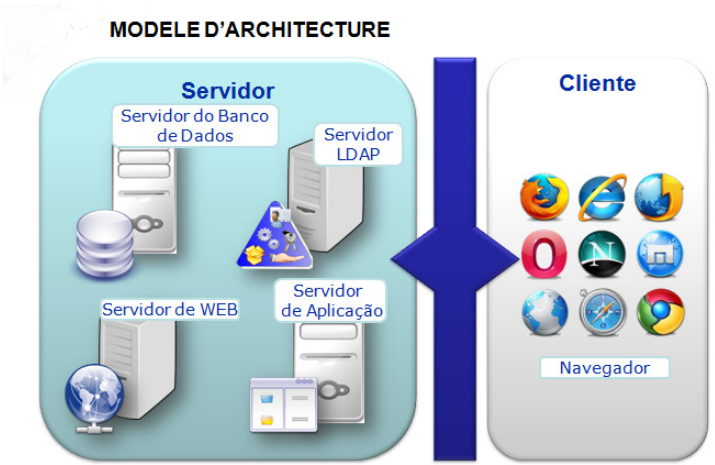


INTECO, como coordenador do CloudCERT Projeto, é o responsável final para completar todos os pacotes de trabalho e do líder de atividades de gerenciamento de projeto.

PT2. DESIGN DA PLATAFORMA

MODELO DE ARQUITETURA

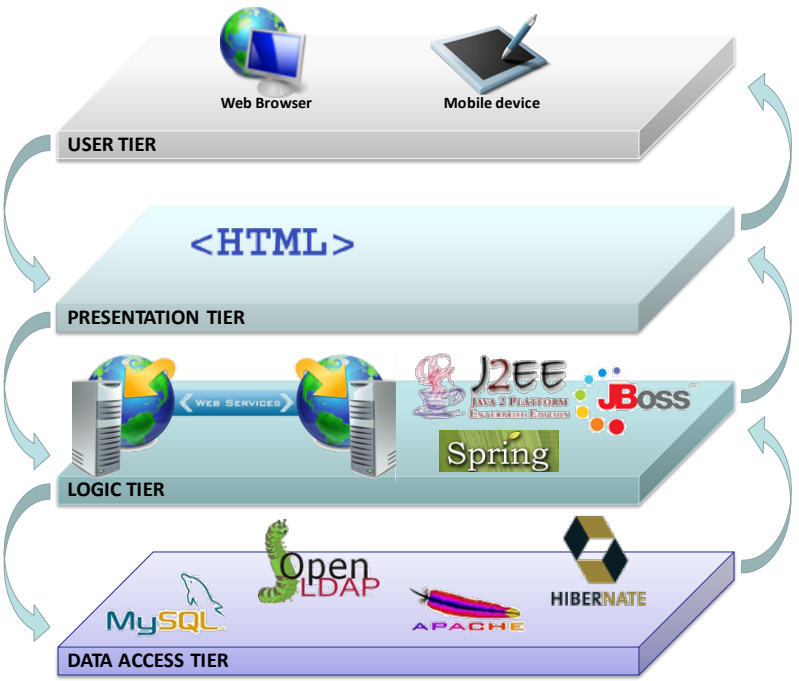
CloudCERT é baseado em uma arquitetura cliente/servidor. O modelo dos diferentes componentes da plataforma CloudCERT baseia-se no padrão J2EE.



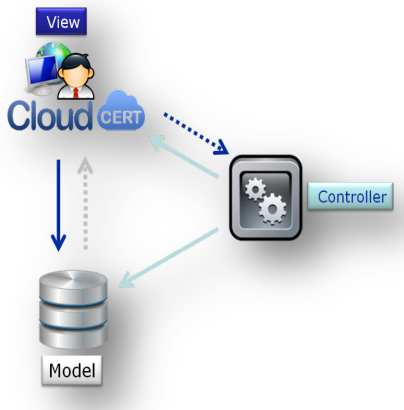
MODELO LÓGICO

Os componentes do modelo lógico da plataforma são agrupados nos seguintes tipos:

- **Persistência de dados**. O CloudCERT tem um modelo de dados complexos. Para lidar com este modelo, alguns Frameworks têm sido usados para gerenciar o modelo de uma maneira eficiente.
- **Aplicações de Segurança**. Todas as tarefas relacionadas com a segurança de aplicativos são baseadas em informações armazenadas em LDAP.
- **Gerenciamento de controle de fluxo da aplicaço.** CloudCERT usa o quadro do Struts. Struts é uma ferramenta de apoio para o desenvolvimento de aplicações Web sob o padrão MVC sob o J2EE plataforma.
- **Serviços de Web**. Eles são implantados em AXIS CloudCERT. AXIS é uma implementação de SOAP desenvolvido pela Apache e OASIS e padrões W3C reunião.
- **Camada de apresentação**. Ele baseia-se na utilização das estruturas: Struts e LDAP.



ESBOÇO DE MVC

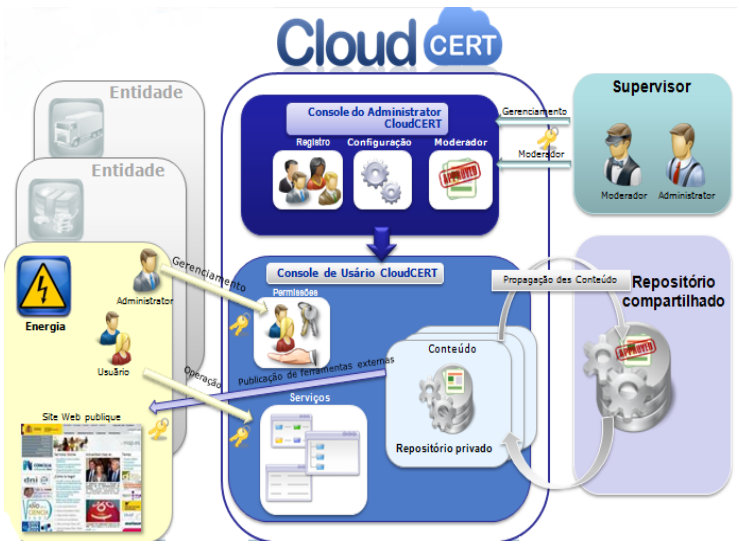


- Como a grande maioria das aplicações J2EE existentes, o modelo - Vista - controlador tem sido adotada na plataforma CloudCERT.

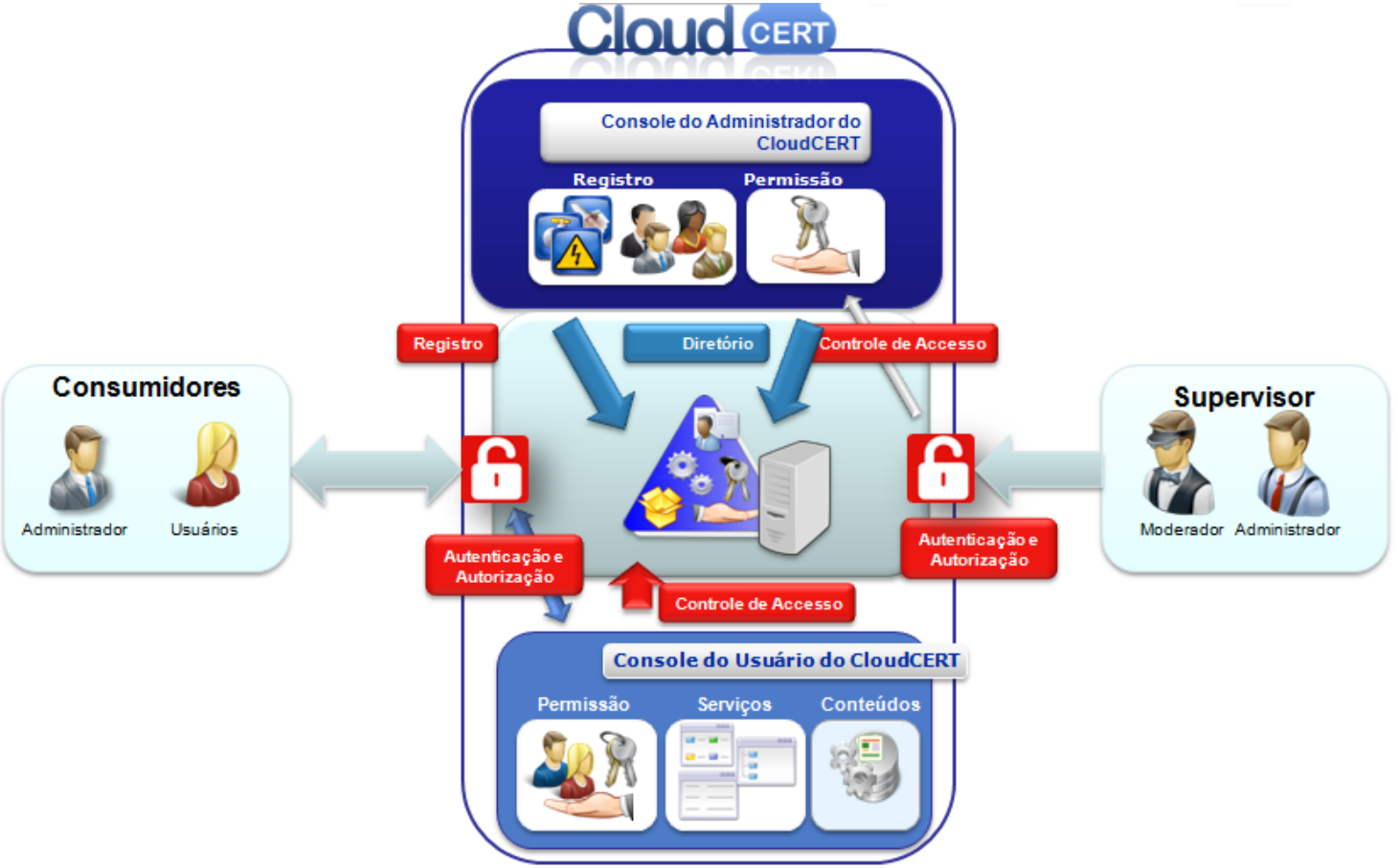
DESIGN FUNCIONAL

Aplicações e módulos que formam a plataforma CloudCERT incluem:

- **Módulo de autenticação do CloudCERT**: Serviço de Autenticação Central (CAS).
- **Módulo de Gerenciamento de senhas**: módulo de gerenciamento de alteração de senha e ativação de contas de usuário.
- **Console do Usuário CloudCERT**: aplicação do console gerencial para diferentes entidades.
- **Console do Administrador do CloudCERT**: gerenciamento de aplicativos para CloudCERT Platform (serviços, serviços web, entidades e conteúdos).
- **Serviços Web CloudCERT.**



SEGURANÇA

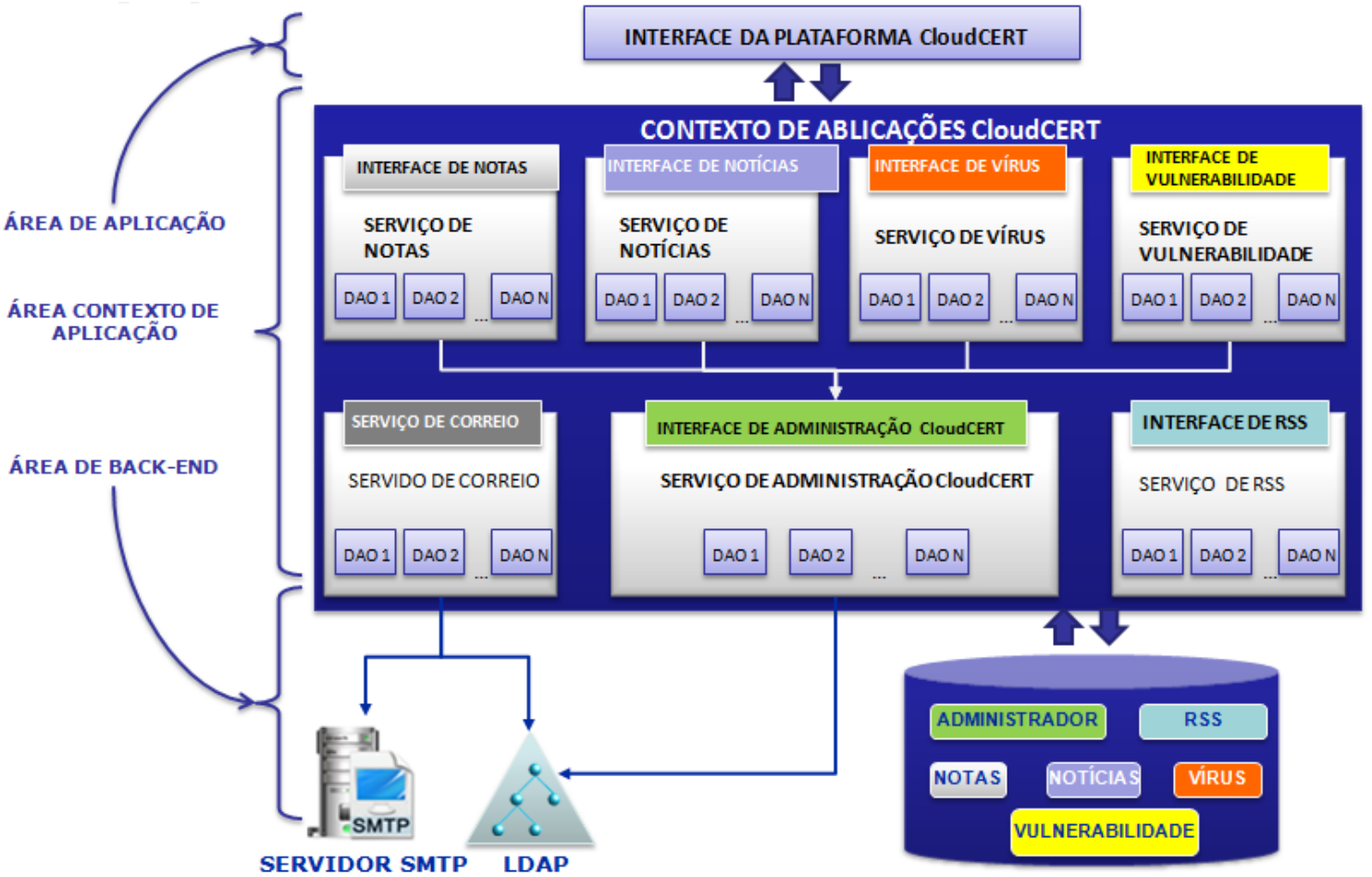


Todas as questões relacionadas com a segurança de aplicativos são baseados em informações armazenadas em LDAP. Os seguintes quadros têm sido usados para gerenciar a segurança CloudCERT:

- **Segurança Spring.** Módulo pertencente ao quadro que permite a lógica do aplicativo para manter o código de segurança gratuito, fornecendo mecanismos de autenticação e autorização para aplicações J2EE. Além disso, a Segurança Spring suporta autenticação no Serviço de Autenticação Central (CAS) fornecendo uma API cliente para interagir com o servidor CAS.
- Módulo **Spring LDAP** pertencente ao quadro e fornece mecanismos de interação para simplificar as operações em qualquer tipo de servidor LDAP.

CONTEXTO GERAL DE DESIGN

Usando a persistencia do banco de dados e LDAP, o CloudCERT definiu um contexto global acessível por diferentes aplicações:



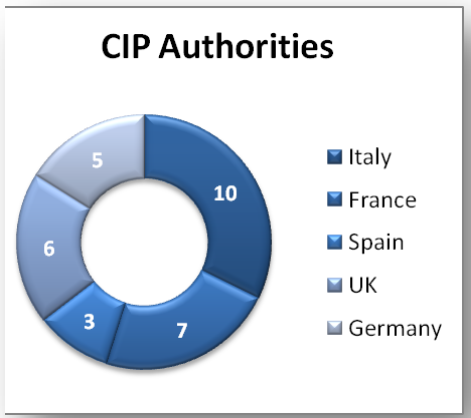
- **Área de Aplicação**. Onde está incluída toda a lógica de apresentação e controle de fluxo.
- **Área de contexto da aplicação**. O contexto que define os diversos serviços oferecidos por uma interface pública para as aplicações que suportam ou outros serviços.
- **Área de Back- End**.
  - Plataforma de Banco de Dados do CloudCERT.
  - CloudCERT LDAP.
  - Servidor SMTP.

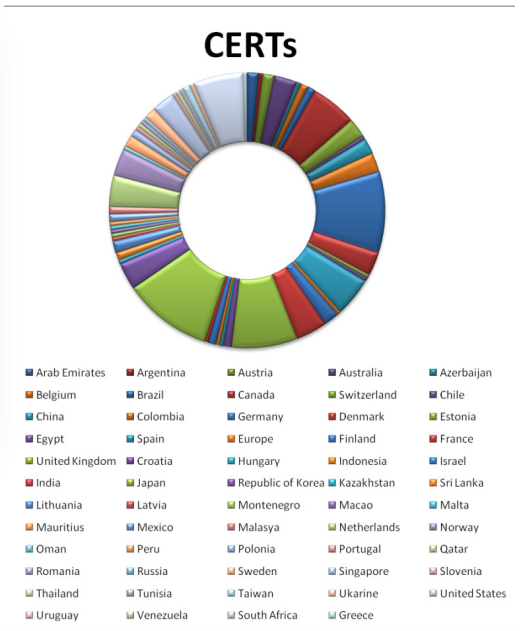
PT3. NORMAS DE INFORMAÇÃO E COMUNICAÇÃO

ONTOLOGIAS DO CONTEÚDO DA INFORMAÇÃO

- **NOTAS**: Gerenciar e compartilhar todas as informações relacionadas a eventos institucionais da "CERT" de interesse geral em rede da plataforma CloudCERT.
- **NOTÍCIAS**: Introduzir, gerenciar e compartilhar todas as notícias públicas que são consideradas de interesse geral.
- **AVISOS**: Introduzir, gerenciar e compartilhar todos os casos considerados como alertas com interesse especial.
- **VÍRUS**: Introduzir, gerenciar e compartilhar todos os vírus de interesse especial.
- **VULNERABILIDADE**: Gerenciar e compartilhar todos essas vulnerabilidades de especial interesse.
- **ITENS RSS**: Confira todos os itens RSS considerados como de especial interesse.

USUÁRIOS POTENCIAIS PARA O CLOUDCERT





PROTOCOLOS E NORMAS DE DESCRIÇÃO E TROCA DE INFORMAÇÕES

FINALIDADES GERAIS DA PARTILHA DE TECNOLOGIAS DE INFORMAÇÃO

- Entre a vasta gama de **protocolos para compartilhamento de informações** que foram desenvolvidos ao longo dos anos, três protocolos foram selecionados em parte por causa de sua ampla utilização em diferentes tipos de organizações, e em parte por causa de sua flexibilidade, que pode ser explorado com sucesso no contexto da o CloudCERT :
  - EDI (Electronic Data Interchange).
  - XML (eXtensible Markup Language).
  - SOAP (Simple Object Access Protocol).

INTERCÂMBIO DE INFORMAÇÕES SOBRE NORMAS ESPECÍFICAS PARA FINS DE SEGURANÇA

O projeto CloudCERT foca especificamente em ajudar os administradores de infraestruturas críticas e infraestruturas críticas de informação para melhor defender-se diante de ameaças de segurança cibernética . As falhas de segurança são (e certamente será no futuro próximo) uma ameaça para a operação de infraestruturas de TI.

Assim que novas falhas são descobertas, informando os usuários e administradores sobre os problemas identificados é uma tarefa vital, tanto para fornecedores de TI e para as equipes de segurança.
A forma mais comum para circular esta informação é por meio de "alertas de segurança", documentos técnicos que descrevem em detalhe as características da emissão, o seu impacto potencial, e muitas vezes também fornecer uma lista de possível solução.

Esta seção enfoca os **formatos padrões** mais populares para as **recomendações de segurança**:

- 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).

PLANO DE SOLUÇÕES ALTERNATIVOS

AVALIAÇÃO DE TROCA DE CONTEÚDO

Índice que incluem informações sobre precioso alertas com interesse especial na rede da CloudCERT são adequados para serem transmitidos com o SOAP (Simple Object Access Protocol) através de HTTPS (Hypertext Transfer Protocol Secure):

- Avisos.
- Vírus.
- Vulnerabilidades.

No entanto, os seguintes conteúdos não são adequados para ser compartilhado:

- N**otas.** Este conteúdo é usado por usuários de CloudCERT para compartilhar informações relacionadas a eventos institucionais CERT em sua própria plataforma de rede.
- **Notícias.** Este conteúdo é usado por usuários de CloudCERT para a partilha de links URL relacionados a notícia pública sem qualquer interesse especial fora a sua própria plataforma de rede dos CERT.
- **Itens RSS.** Este conteúdo é usado por usuários de CloudCERT para compartilhar itens RSS a partir de diferentes *feeds* públicos.

INDICADORES

É importante gerenciar cuidadosamente todo o conteúdo que compartilham com outras organizações. Para este fim, um módulo de painel foi sido necessário integrar a Plataforma CloudCERT permitindo ao administrador para patrulhar um conjunto de indicadores relacionados a esta atividade.

Os indicadores identificados adequados a serem monitorados foram:

- Número de elementos produzidos durante um período de tempo específico.
- Número de elementos lidos durante um período de tempo especificado.
- Top N conteúdos mais lidos.
- As organizações Top N produtores mais ativos.
- As organizações Top N leitores mais ativos.
- As organizações Top N mais ativo importar conteúdo (a partir de repositório compartilhado com o próprio repositório).
- Distribuição mensal da maioria dos dias ativos de produção/consumir conteúdo.

PT4. QUADRO DE DEFINIÇÃO SEGURO

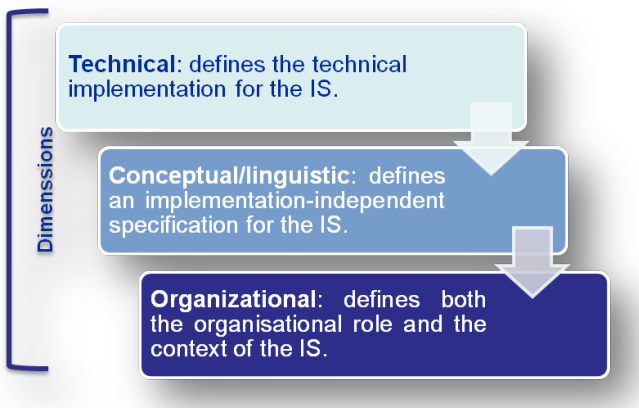
PRÁTICAS DE TRABALHO PARA GESTÃO SEGURO E COMPARTILHAMENTO DE INFORMAÇÕES SENSÍVEIS

A plataforma CloudCERT se destina a facilitar o intercâmbio de **informações sensíveis** sobre CIP através de vários tipos de partes interessadas com todas as garantias de segurança. Daí a primeira atividade do pacote de trabalho ser uma pesquisa para investigar as práticas de trabalho para o manuseio seguro e compartilhamento de informações confidenciais.

SEGURANÇA DA INFORMAÇÃO

Neste capítulo, o domínio de suas principais questões associadas, com um foco particular sobre os Sistemas de Informação de segurança e informação é introduzida.

- **Confidencialidade**: divulgação indevida de informações deve ser detectada e evitada.
- **Integridade**: a informação não deve ser modificada, por sujeitos não autorizados.
- **Disponibilidade**: a informação deve estar disponível a indivíduos autorizados sempre que necessário.



COMPARTILHAMENTO DE INFORMAÇÕES PARA CIP

Este capítulo analisa o que foi feito para permitir a partilha de informação eficaz, dentro do contexto da CIP, pelos governos de dois dos países mais importantes do mundo: os Estados Unidos e o Reino Unido.

PROTEÇÃO DAS INFRAESTRUTURAS CRÍTICA

Dois países foram tomados como exemplo e os seus planos CIP descrito e analisado em detalhes: as políticas elaboradas pelos Estados Unidos e a situação italiana:

- Estratégia Nacional para a Segurança Interna.
- Quadro Estratégico Nacional da Itália para a segurança do ciberespaço.

REQUERIMENTOS DE SEGURAÇA DO CLOUDCERT

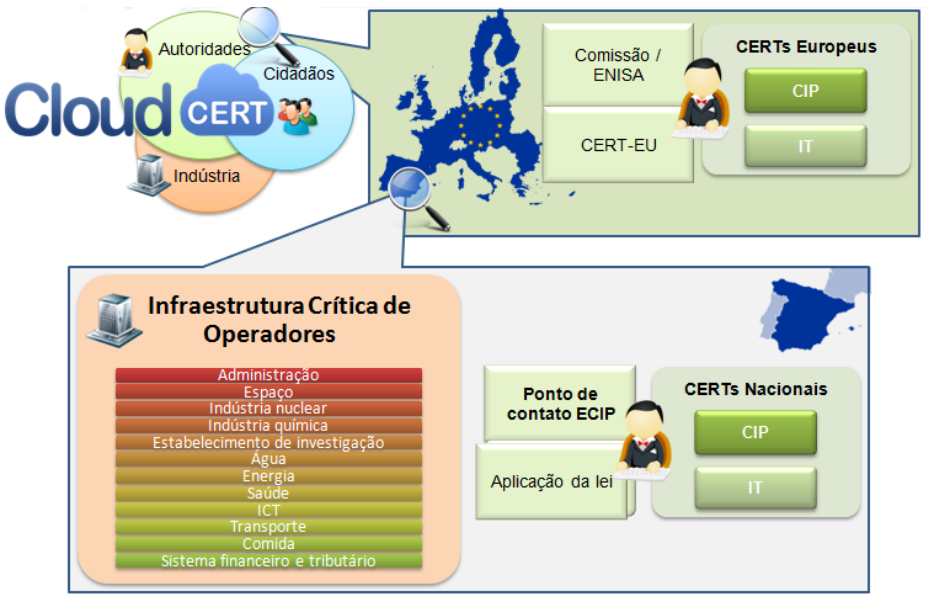
Os principais objetivos destas entregas são:

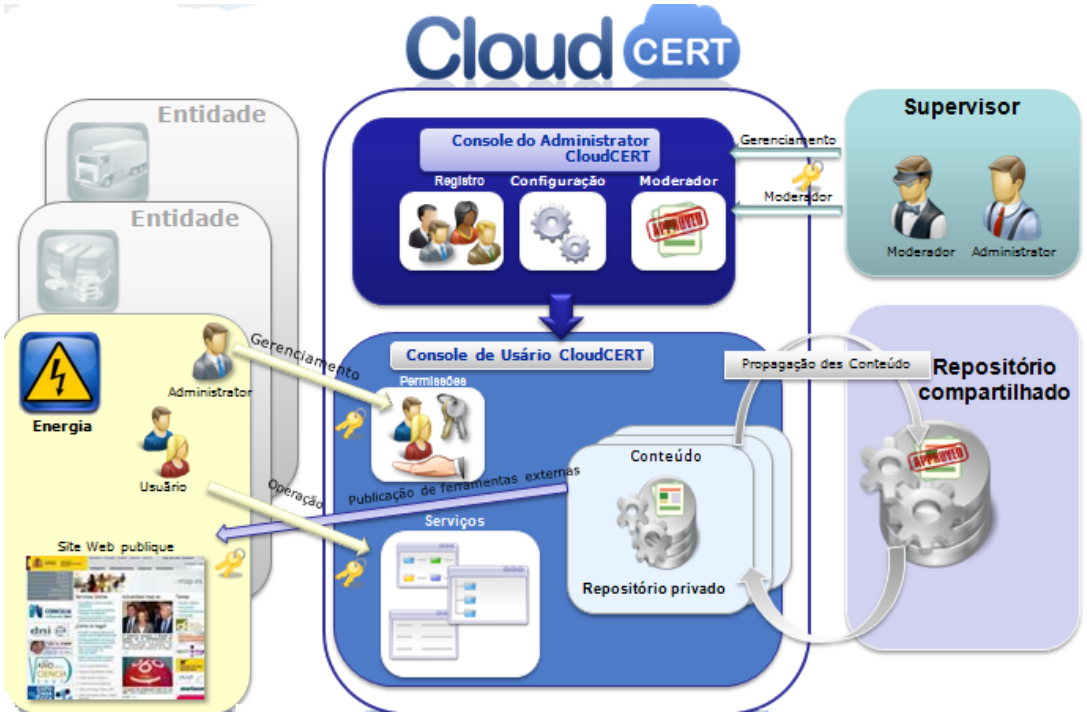
- Identificar as principais fontes científicas no campo da PIC.
- Identificar métodos e procedimentos hipotéticos para ampliar e fortalecer processos colaborativos do sistema.
- Identificar métodos e procedimentos hipotéticos que permitam ampliar e fortalecer a capacidade de coordenação entre os *stakeholders* do sistema durante todo o ciclo de vida do IC hipotéticas.

Tudo com o objetivo final de atualização do modelo operacional da governança, a fim de atribuir funções, responsabilidades e objetivos dos *stakeholders* do sistema.

Os *stakeholders* CloudCERT são agrupados em três categorias principais:

- **Autoridades (setor público):** autoridades competentes em segurança da informação e à proteção da infraestrutura crítica, incluindo a nível legal e operacional. Nisto inclui políticas e indicadores bem como equipes de aplicação da lei.
- **Indústria (setor privado):** operadores de infraestruturas críticas, incluindo os principais fornecedores (Desenvolvedores e fabricantes de produtos e serviços).
- **Cidadãos (público-alvo):** os consumidores dos serviços prestados pela infraestrutura crítica.





Os *Stakeholders* interagem com a plataforma CloudCERT baseado em um modelo de governança regulados conforme descrito abaixo:

- Diferentes **entidades** podem acessar a Plataforma: CERT, equipes de de aplicação da lei e operadores de infraestruturas críticas. Cada entidade tem seu próprio espaço para alocar o conteúdo e pode importar conteúdo do repositório compartilhado. Eles podem exportar automaticamente conteúdo para ferramentas externas, como seu próprio site interno.
- **A organização supervisora**:
  - Faz a **gestão** da plataforma por organizações e assim registrar seu usuário administrador, bem como por configurar e gerenciar os serviços disponíveis. A Supervisora configura permissões de entidades de conteúdos e serviços contratados.
  - Suprimentos de **moderação**. Todos os conteúdos para fazer parte do **repositório compartilhado** devem ser propagados pela supervisora. Moderação também envolve publicações em ferramentas como fóruns, wiki, etc.
- Cada entidade tem um **usuário de administração** que pode criar usuários e atribuir permissões para sua entidade. O Conteúdo do repositório privado da entidade pode ser publicado em um repositório compartilhado com a aprovação do supervisor.
- s **usuários** podem interagir com os conteúdos e serviços da plataforma.

PT5. DEVELOPMENT DA PLATAFORMA

Durante esta fase é implementado o projeto-piloto. Para este efeito, as seguintes tarefas são realizadas:

ANÁLISE E REQUISITOS

A especificação de requisitos de software tem como objetivos:

- Identificar, pedindo que os usuários finais, os requisitos e funcionalidades da plataforma CloudCERT.
- Incorporar as exigências da estrutura de segurança e troca de informações sensíveis.
- Definir e priorizar os requisitos para a plataforma CloudCERT.

DESENVOLVIMENTO

Seguindo a ágil metodologia do **Scrum**, a fase de desenvolvimento inclui:

- Implementação dos requisitos adquiridos na fase anterior, para criar um piloto funcional.
- Criação da documentação do usuário e administração do piloto desenvolvido.

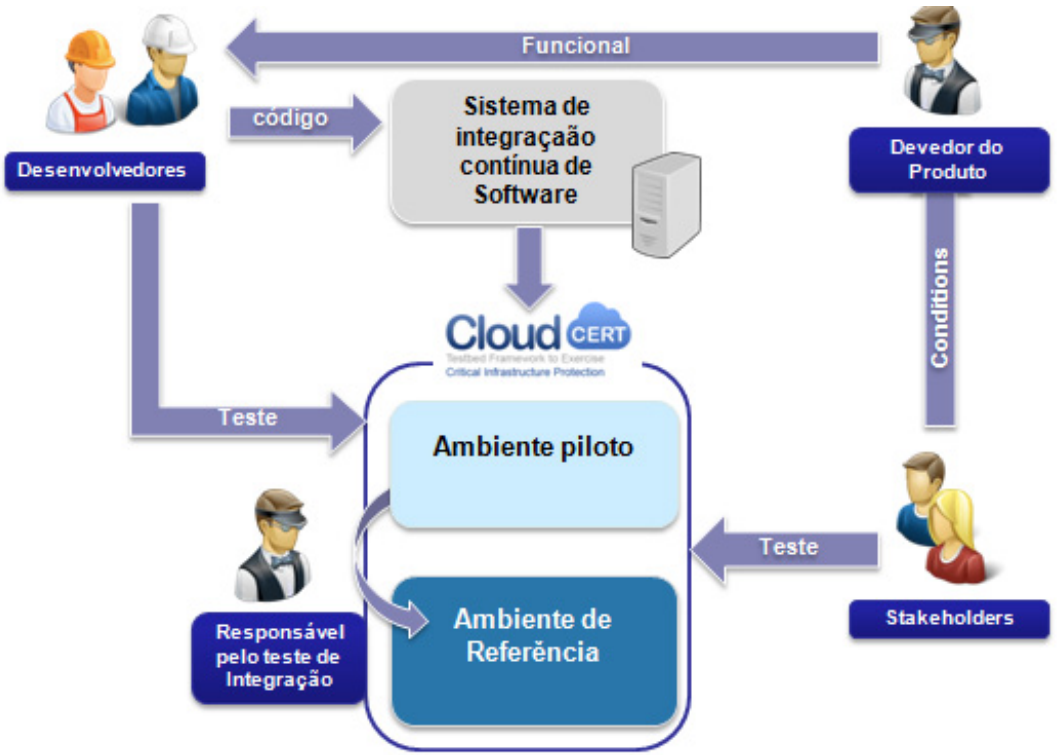
CONFIGURAÇÃO DA PLATAFORMA

Durante esta fase, os ambientes de desenvolvimento e teste são fornecidos e também manuais de instalação da configuração são criados.

AMBIENTE

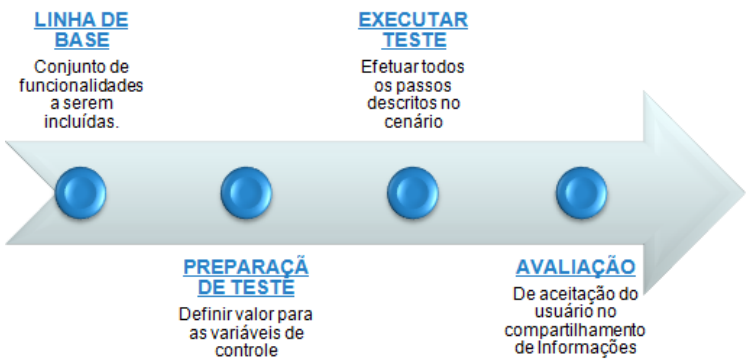
Ambiente piloto é usado para carregar e testar novos desenvolvimentos, e verificá-los depois de cada *sprint*.

Quando a fase de testes termina e tudo foi verificado, a nova versão é implantada em **ambiente de referência**, que contém uma versão mais estável da Plataforma CloudCERT.



PT6. EXPERIMENTAÇÃO PILOTO

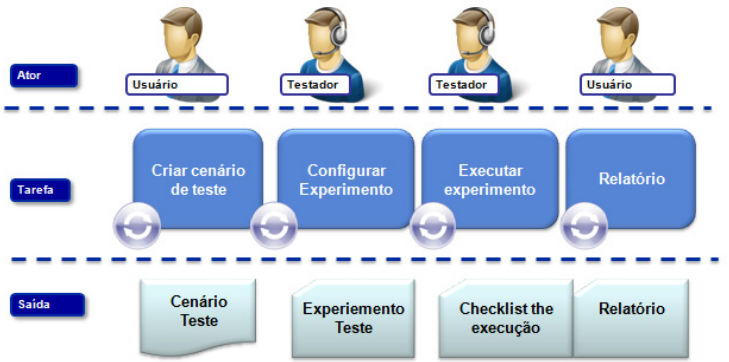
As atividades PT6 estão focadas em experimentação e avaliação com base nos casos de usuários de integração, sobre a Plataforma Piloto desenvolvido e instalado em PTs anteriores. As atividades incluem testes funcionais e de aceitação do produto, bem como exercícios de simulação para a troca de informações entre os usuários da plataforma para experimentar e demonstrar em casos simulados, a troca de informações sobre a descoberta de vulnerabilidades, alertas de segurança e avisos e relatar incidentes de segurança.

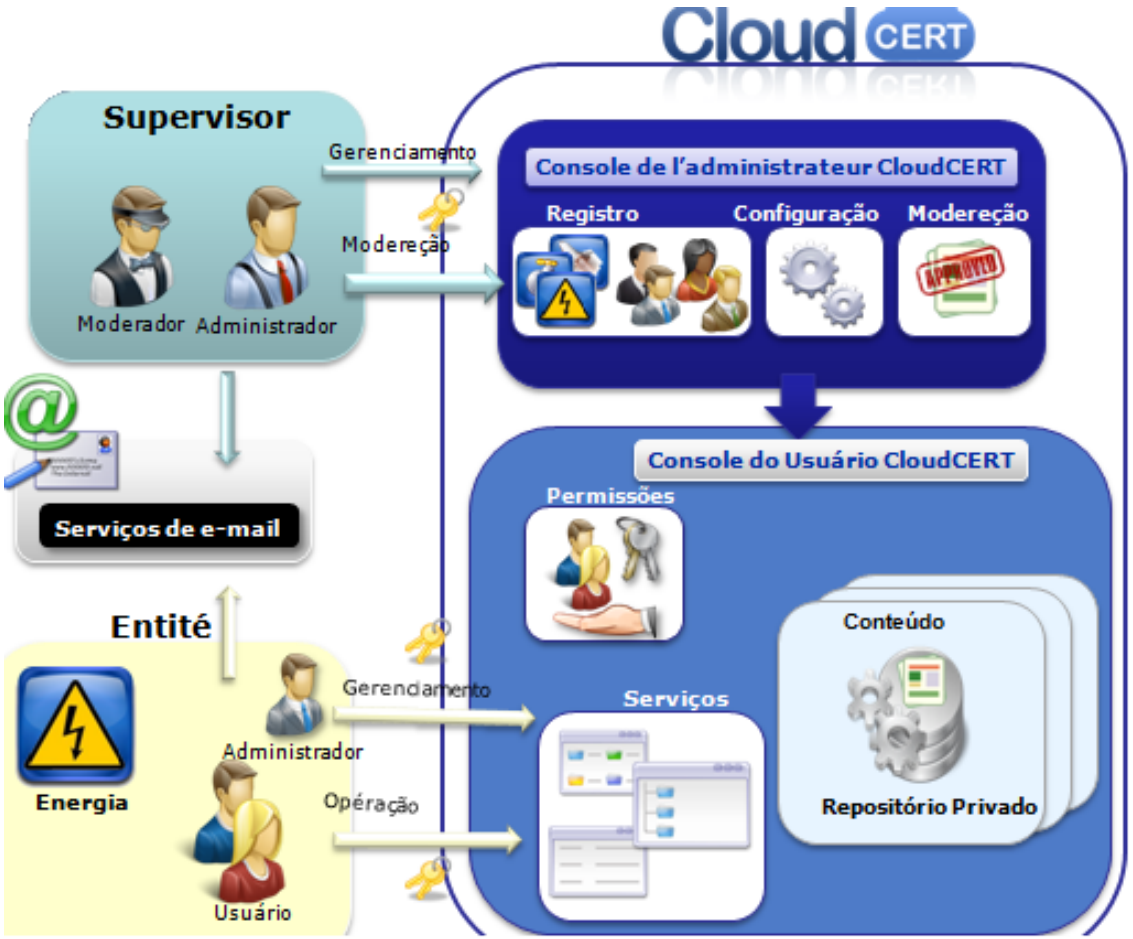


O destino da avaliação e experimento é usar e cenário de experimentação como uma base para avaliar a contribuição da solução de plataforma CloudCERT para melhorar a colaboração e cooperação entre os atores do CIP na partilha de informações de segurança cibernética, e assim testar a funcionalidade e de trabalho disponível para a comunicação flui de ser realizada.

Para fins da avaliação, os resultados da experimentação, se baseada nas seguintes categorias:

- CloudCERT teste (se os processos de compartilhamento de informações estão corretamente suportada);
- verifica o quanto CloudCERT aborda os desafios e necessidades do domínio em termos de colaboração e cooperação;
- avaliar o potencial melhoria no CIP ativado por CloudCERT





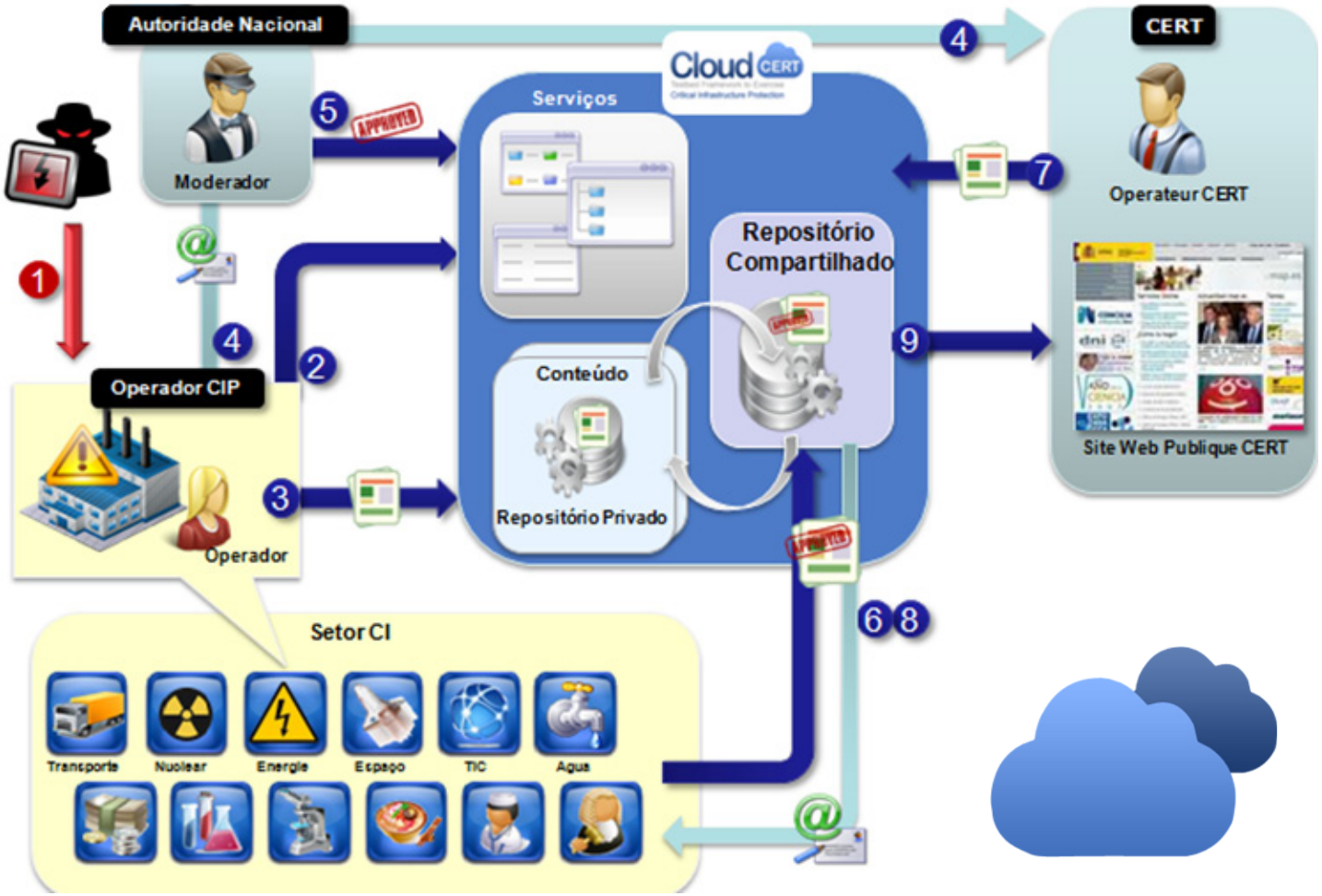
FERRAMENTAS PARA EXPERIMENTAÇÃO

- **Console de Administração do CloudCERT.** Permite toda a gestão das funcionalidades da plataforma CloudCERT.
- **Console de Usuário do CloudCERT**. Facilita a criação, implantação e operação de novas entidades para dar resposta em incidentes de segurança.
- **Ferramenta de cliente de e-mail.**

ATORES

- Usuário - CI Operador
- Administrador - CI Operador
- Moderador - CERT/Autoridade
- Administrador - Autoridade

CASO DO USUÁRIO EM CENÁRIO DE EXEMPLO



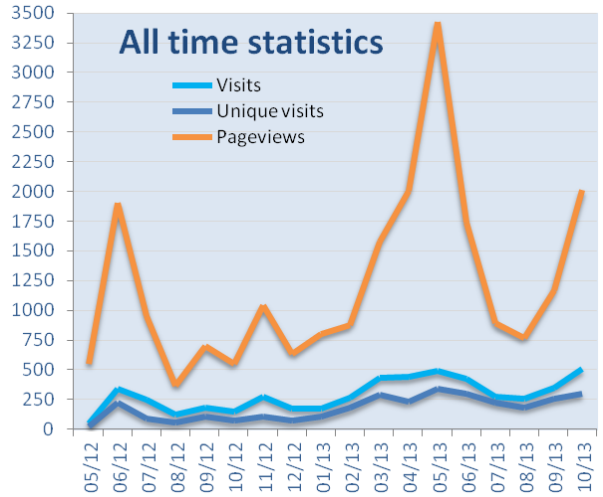
1. Operador **detecta uma vulnerabilidade** de um produto e de intrusão em rede interna.
2. Pesquisas de informação e leituras **procedimento para lidar com incidentes** em wikiCIP.
3. Cria um **aviso** e **mensagens** no Fórum.
4. **Comunicação** oficial de Incidentes.
5. CNPIC **valida** o aviso.
6. **e 8.** Aviso visível na CloudCERT e por e-mail através do boletim.
7. CERT **resolve** o aviso e fecha o post do Fórum com uma solução alternativa.

9 Aviso é publicado em um **site externo**.

PT7. DIVULGAÇÃO DOS RESULTADOS DO PROJETO

A maioria dos indicadores relevantes do site do projeto CloudCERT **http://cloudcert.european-project.eu/** :

- Mais de **200** notícias publicadas.
- Mais de **5.000** visitas (acumulado).
- Mais de **40** recursos compartilhados.
- Mais de **22.000** *pageviews* (acumulados).



WIKIPEDIA

- Inglês: http://en.wikipedia.org/wiki/CloudCERT
- Espanhol:http://es.wikipedia.org/wiki/CloudCERT
- Italiano: http://it.wikipedia.org/wiki/CloudCERT

EVENTOS

2012

- Conferência CRITIS12 sobre Segurança Informações de Infraestruturas de Criticas http://critis12.hig.no/.

2013

- Semana de Inovação para Jovens Investigadores
- 8 ª Oficina ENISA CERT.
- 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


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 454.952,73 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 Puckas Foundation (HU).

Raúl Rivas / Ignacio Cano

CONFERÊNCIA FINAL

A Conferência final da CloudCERT serviu para divulgar os resultados do projeto europeu para o público-alvo.

- **Data**: 22 de novembro de 2013.
- **Localização:**
  - Madri na Espanha, no espaço da Secretária de Estado das Telecomunicações e da Sociedade da Informação (SETSI).
- **Público-alvo:**
  - Os stakeholdres do projeto CloudCERT.
  - Os operadores de infraestruturas críticas espanholas, incluindo fornecedores principais dos fornecedores.
  - Outros CERT européias e as equipes de aplicação da lei, envolvidos no CIP.
- **Admissão:**
  - Entrada gratuita por convite e transmitido via streaming de vídeo. http://www.cloudcert.webcastlive.es.

SOLUÇÃO TECNOLÓGICA

PLATAFORMA COLABORATIVA

A CLOUDCERT PODE SER INTERESSANTE PARA VOCÊ?

- Se a sua organização é um **CERT** ou um **operador de CI**, você pode usar esta plataforma para lidar com incidentes de infraestruturas críticas e compartilhar informações de segurança cibernética.
- Se a sua organização constitui como **CERT** ou **Autoridade** e inclui **operadores de infraestruturas críticas**, você pode obter uma plataforma de personalizada para prestação de serviços e ferramentas para a sua infraestrutura crítica proteção eleitorado (fórum, wiki, etc).
- Se a sua organização tem de interagir com as **Autoridades Nacionais de Proteção das infraestruturas**, e dependendo de suas competências nacionais você pode atribuir dentro da plataforma, o papel mais adequado: a coordenação, a supervisão, participação, etc.

CONTEÚDOS

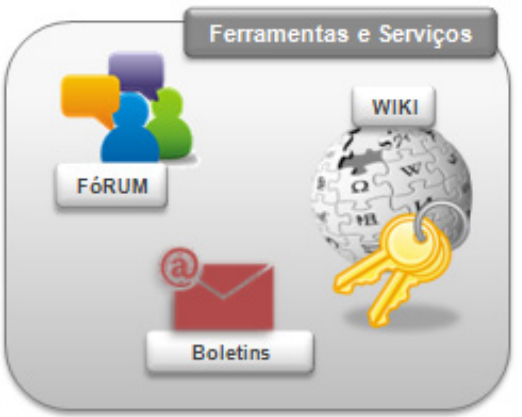
A plataforma CloudCERT permite criar e propagar conteúdos de segurança, tais como:

- Notas.
- Notícias.
- Avisos.
- Vírus.
- Vulnerabilidades.
- Itens RSS.

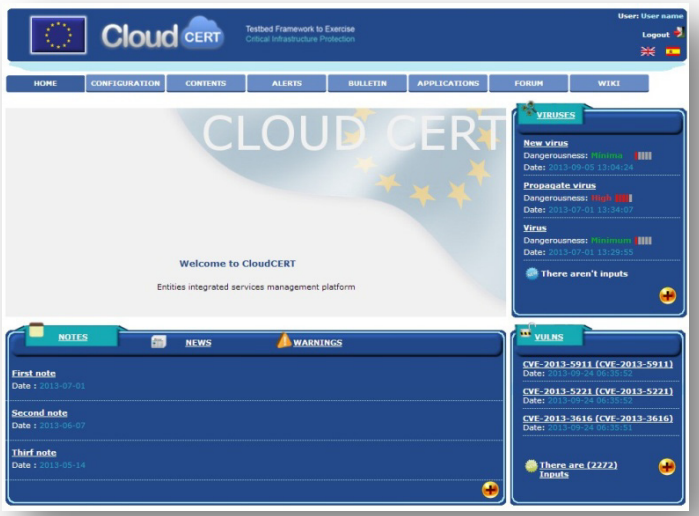
SERVIÇOS E FERRAMENTAS

A plataforma CloudCERT permite que os usuários compartilhem informações para prevenir incidentes de segurança através de seus serviços:

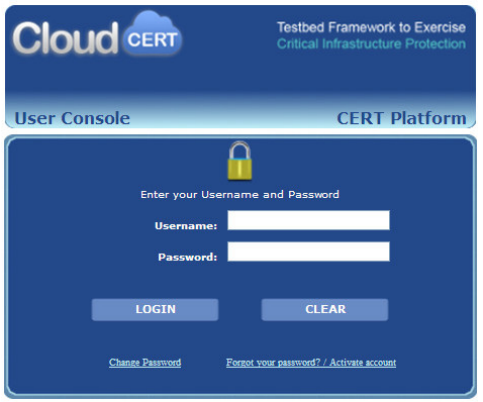
- Fórum.
- WikiCIP.
- Boletins de Serviço.



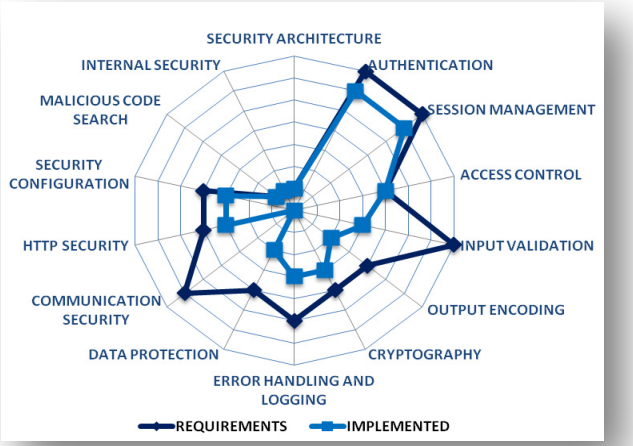
FOLHA DE DADOS



- A **Plataforma colaborativa** para gerenciar um repositório compartilhado de informações de segurança cibernética para cooperar de uma forma eficiente.



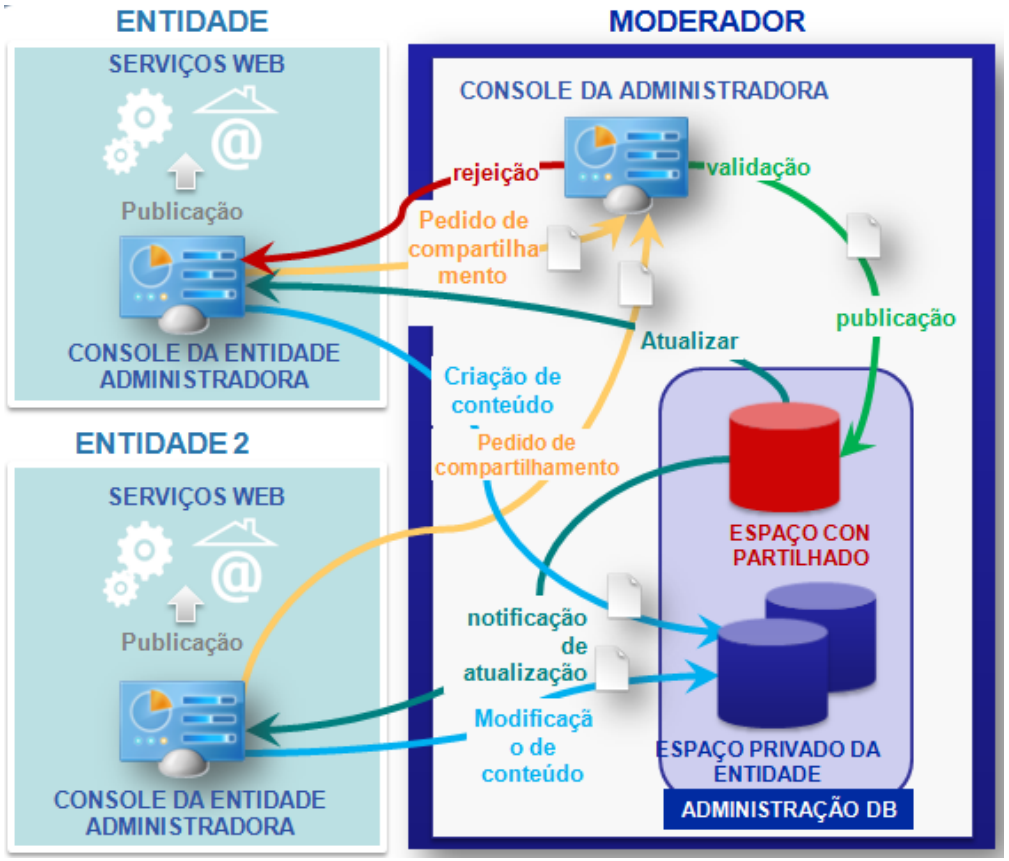
- **Cloud** paradigma baseado em repositórios privados e partilhados.
- Aplicação **multi-idioma** da interface e conteúdo de tradução.
- **Serviços** personalizados (contratado).
- Plataforma em **escala** que permite que novos conteúdos, serviços, ferramentas e fluxos de trabalho.
- **Ambiente seguro:**
  - Mecanismo de autenticação baseada em nome de usuário e senha: Authentication Service Central (CAS).
  - A autorização baseada em permissões e função.
  - Gestão de sessões seguras.
  - Confidencialidade e proteção de dados garantida.



CICLO DE VIDA DO CONTEÚDO

- A CloudCERT permite **criar** e **atualizar** conteúdo (informação estruturada) de modo colaborativo.
- Cada entidade mantém o conteúdo em seu próprio **espaço privado** e poderá solicitar para a partilha.
- Um moderador opiniões conteúdo a ser publicado em um **repositório compartilhado.**
- Entidades podem **recuperar** seu conteúdo a ser publicado em ferramentas externas (como intranets).

Criar / Modificar um conteúdo: Azul
Pedido de Partilha: Amarelo
Atualizar um conteúdo: Verde Escuro
Pedido de Validação: Verde Claro
Pedido Rejeição: Vermelho

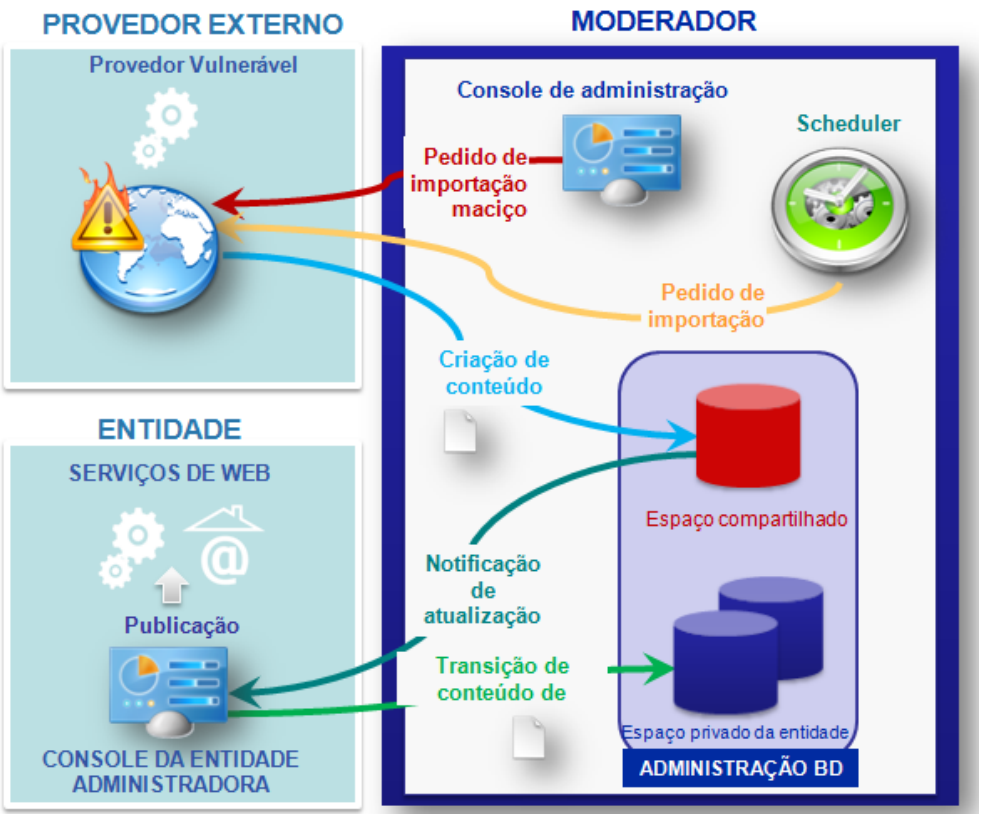


O conteúdo pode estar nos seguintes estados durante seu ciclo de vida:

- Criado.
- Modificado
- Compartilhado.
- Atualizado.
- Validado.
- Rejeitado.

VULNERABILIDADE DO CICLO DE VIDA

- As vulnerabilidades são um tipo específico de conteúdo fornecido por **fontes externas** (como o NIST).
- Uma tarefa agendada **importa** automaticamente as vulnerabilidades no sistema.
- Moderador também pode **solicitar uma massiva importação** (por um período de tempo) no sistema.
- Entidades podem **traduzir vulnerabilidades** em seu próprio espaço privado.



Vulnerabilidade de armazenamento: Azul
Pedido de incrementação da importação: Amarelo
Notificação de atualização: Verde Escuro
Tradução de vulnerabilidade: Verde Claro
Pedido de importação maciço: Vermelho

Portanto, uma vulnerabilidade pode estar nos seguintes estados durante o seu ciclo de vida:

- Importado.
- Notificado (atualização).
- Traduzido.

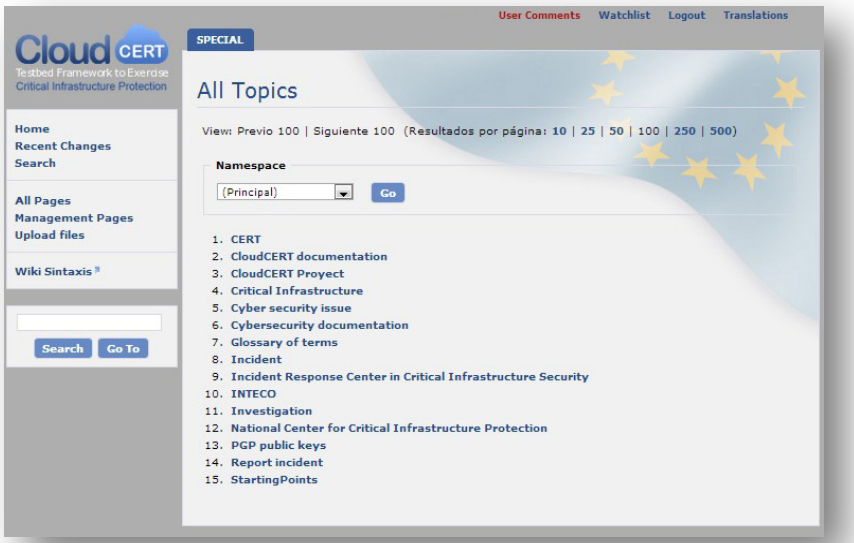
WIKICIP

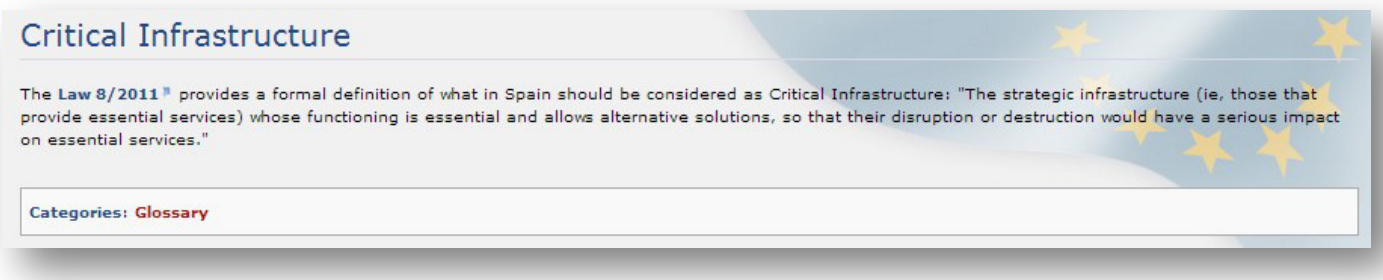
Um wiki é um sistema flexível e permite ao administrador definir qualquer hierarquia da página. WikiCIP permite a manutenção de **conteúdos não estruturados** de maneira colaborativa com os seguintes elementos de estrutura disponíveis:

- **Índice** – A Página de índice que exibe links para diferentes páginas wiki com um tópico similar.
  - **Página** – As páginas individuais sobre um tópico específico.

WikiCIP tem estrutura os seguintes tópicos:

- **A documentação do CloudCERT**:
  - Apresentação genérica do projeto e os principais recursos.
    - Manual do usuário.
    - Manual do Administrador.
    - Manual do Desenvolvedor.
- **Documentação de Segurança Cibernética:**
  - Processo de operação aos incidentes de segurança cibernética.
  - Quadro jurídico.
  - Links interessantes de CIP.
- **Glossário.** Principais termos relacionados com a proteção das infraestruturas.

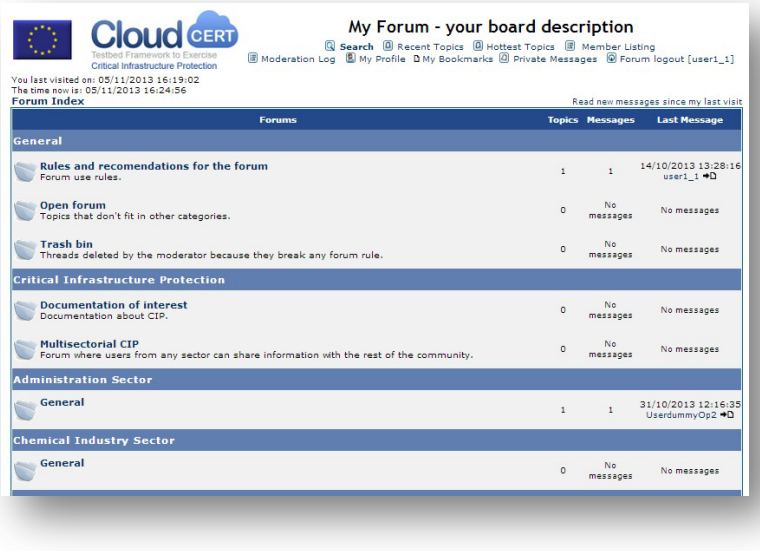




FÓRUM

The forum service allows unstructured information exchange with the following grouping elements available:

- **Categoria.** É o elemento mais alto da hierarquia e normalmente usado para agrupar vários fóruns relacionados. Esse é um grupo lógico, assim sempre no interior de um fórum a categoria tem seu próprio ciclo de vida.
  - **Fórum**. Um fórum é um grupo de ameaças ou debates sobre o mesmo tema.
    - **Tópico** ou **Tema**. É o próprio debate em si, as mensagens dos usuários, falando sobre um tópico específico.



O Fórum do CloudCERT tem as seguintes categorias:

- **Geral**. Fóruns para informações gerais.
- **Proteção das Infraestruturas Críticas.** Onde os usuários podem discutir e compartilhar informações gerais sobre a proteção da infraestrutura crítica com o resto da comunidade.
- Cada operador de infraestrutura crítica tem um fórum reservado para seu **setor** (de acordo com a CIP Espanhol classificação da legislação nacional), onde os usuários podem compartilhar informações com outros atores relevantes no setor.
  - Administração.
  - Espaço.
  - Indústria Nuclear.
  - Indústria Química.
  - Estabelecimento de Investigação.
  - Água.
  - Energia.
  - Saúde.
  - Tecnologia de Comunicações da Informação. (ICT)
  - Transporte.
  - Alimentos.
  - Sistema Financeiro e Tributário.

BOLETINS DE SERVIÇO

A Boletins de Serviço é um serviço externo que se comunica com a Plataforma CloudCERT para **receber inscrições de usuários** e **obter conteúdos de segurança armazenados** em bancos de dados CloudCERT para criar os boletins. Boletins de Serviço é responsável pela criação e formatação dos boletins, e entregar os boletins para os usuários finais de acordo com suas preferências.

Cada entidade registrada CloudCERT, podem se inscrever os usuários (usuários previamente cadastrados ou usuários externos) para diferentes boletins de segurança (*newsletters*), a fim de receber os boletins periodicamente para suas caixas de entrada de e-mail.

A assinatura pode ser processada pelo administrador da entidade ou pelo usuário final.

- Boletins de Serviço permite que os usuários sejam informados sobre as atualizações de conteúdo através de notificações por email.
- Um processo de subscrição para selecionar o tipo e conteúdo de boletim é necessário.
- O serviço de boletins recolhe conteúdos, cria os boletins personalizados e oferece a cada usuário final.

Cloud CERT

Testbed Framework to Exercise
Critical Infrastructure Protection

CloudCERT - Quadro de banco de ensaio para exercício de proteção de infraestrutura crítica.

HOME/2010/CIPS/AG/20.
Com o apoio financeiro da Prevenção, preparação e gestão das consequências em matéria de terrorismo e outros riscos relacionados com a segurança do programa. Comissão Europeia - Direção-Geral de Justiça, Liberdade e Segurança.