

Interoperabilidad Ingeniería Biomédica

CDA - FHIR

Sesión 4

Ing. Pedro Ortiz Tamayo



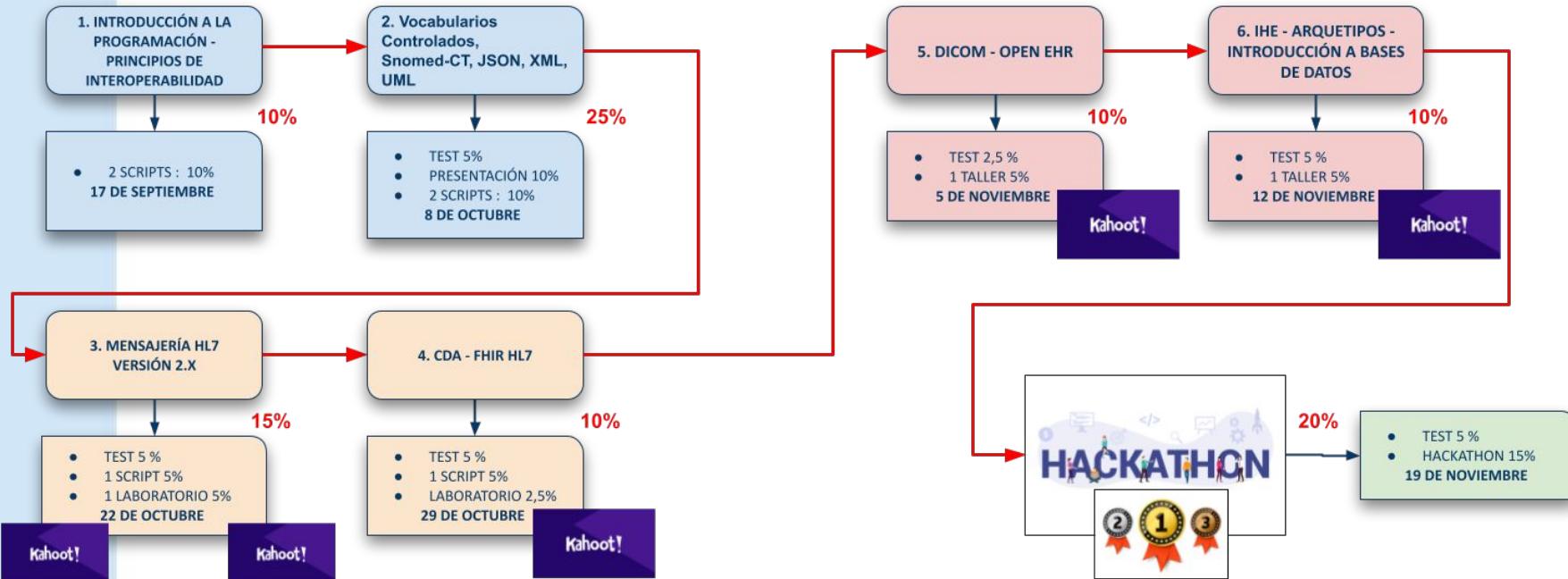
UNIVERSIDAD CES
Un compromiso con la excelencia

La Universidad CES es la propietaria y titular de todos los derechos de propiedad intelectual asociados al presente contenido. La comunicación pública del mismo se realiza, única y exclusivamente, con fines de divulgación e información. Por lo tanto, el material no se podrá usar para propósitos diferentes a los indicados.

La presente divulgación no implica licencia, cesión o autorización de uso o explotación de ningún tipo de derechos de propiedad intelectual diferentes sobre el mismo. La copia, reproducción total o parcial, modificación, adaptación, traducción o distribución, infringe los derechos de la Universidad y causa daños por los que se podrá ser objeto de las acciones civiles y penales correspondientes y de las medidas cautelares que se consideren pertinentes o necesarias. Las opiniones expresadas por los autores o participes no constituyen ni comprometen la posición oficial o institucional de la Universidad CES.



PLAN DE TRABAJO INTEROPERABILIDAD - INGENIERÍA BIOMÉDICA





Open Networking Lab

Envío y Recepción de Mensajes HL7



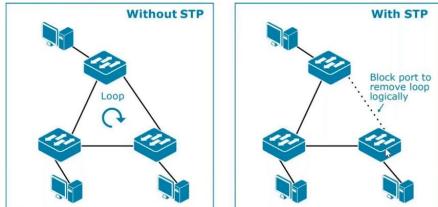
UNIVERSIDAD CES
Un compromiso con la excelencia

Que es Spanning Tree?

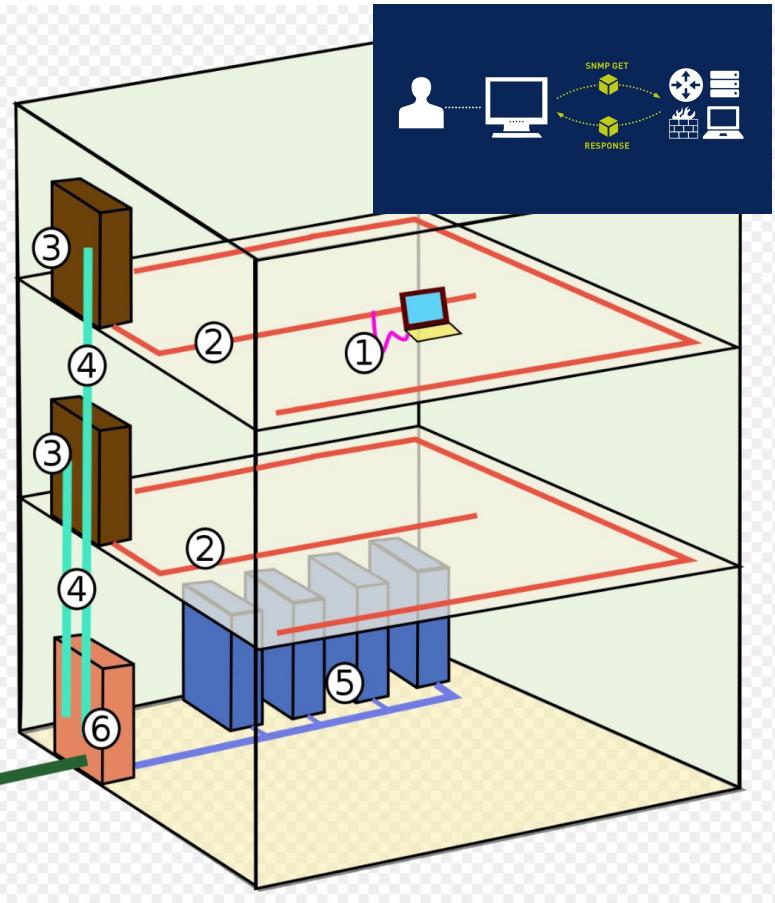
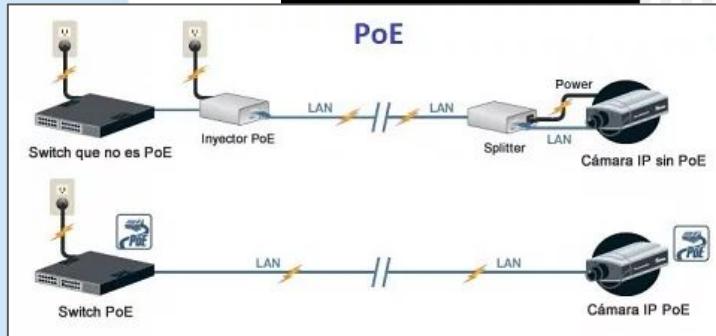


Evitar Loop

- El protocolo Spanning Tree puede resolver los problemas de Loop.



D-Link

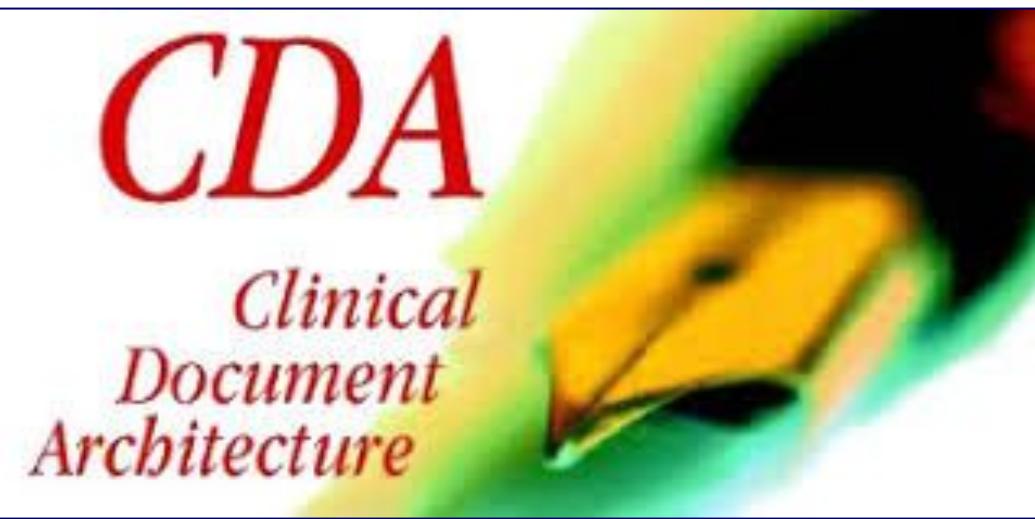


Subsistemas del cableado estructurado: 1- Cableado de área de trabajo 2- Cableado horizontal 3- Cableado de administración (armario de cableado, rack) 4- Cableado vertical (central, backbone) 5- Centro de cálculo 6- Cableado de equipamiento (armario de entrada al edificio) 7- Cableado del campus (acometida, cableado entre edificios)

CONTENIDO SESIÓN 5:

1. HL7 Ver. 3 CDA
 - 1.1. RIM
 - 1.2. Historia
 - 1.3. Características
 - 1.4. Alcance
 - 1.5. Objetivos
 - 1.6. Estructura
2. HL7 FHIR
 - 2.1. Porque FHIR?
 - 2.2. Alcance
 - 2.3. Recurso
 - 2.4. Rest





HL7 v3: CDA



UNIVERSIDAD CES
Un compromiso con la excelencia

HL7 Ver.3 CDA

Los documentos son objetos que el médico está acostumbrado a intercambiar por ejemplo, epicrisis, informes de alta, interconsultas, etc., solo que hoy no utiliza un formato estandarizado. Los documentos reflejan la forma histórica del registro médico y permiten mezclar texto narrativo libre con información estructurada. También, los documentos posibilitan la firma del responsable, como sucede en papel (en este caso, firma digital). Los documentos conllevan información completa : no son divisibles. Alcanza con un documento para representar por completo el acto médico asociado.



HL7 Ver.3 CDA

CDA es la abreviatura de Clinical Document Architecture, una especificación para intercambio de documentos que utiliza XML, el modelo de información de HL7 (RIM), la metodología de HL7 v3 y vocabularios controlados o locales (SNOMED, ICD, LOINC, etc.). Define el marcado de documentos para especificar la semántica y la estructura. CDA puede usarse de manera tan simple o compleja como se requiera o se pueda pagar: desde enviar un documento con información contextual mínima, hasta otro completamente codificado y referenciado.

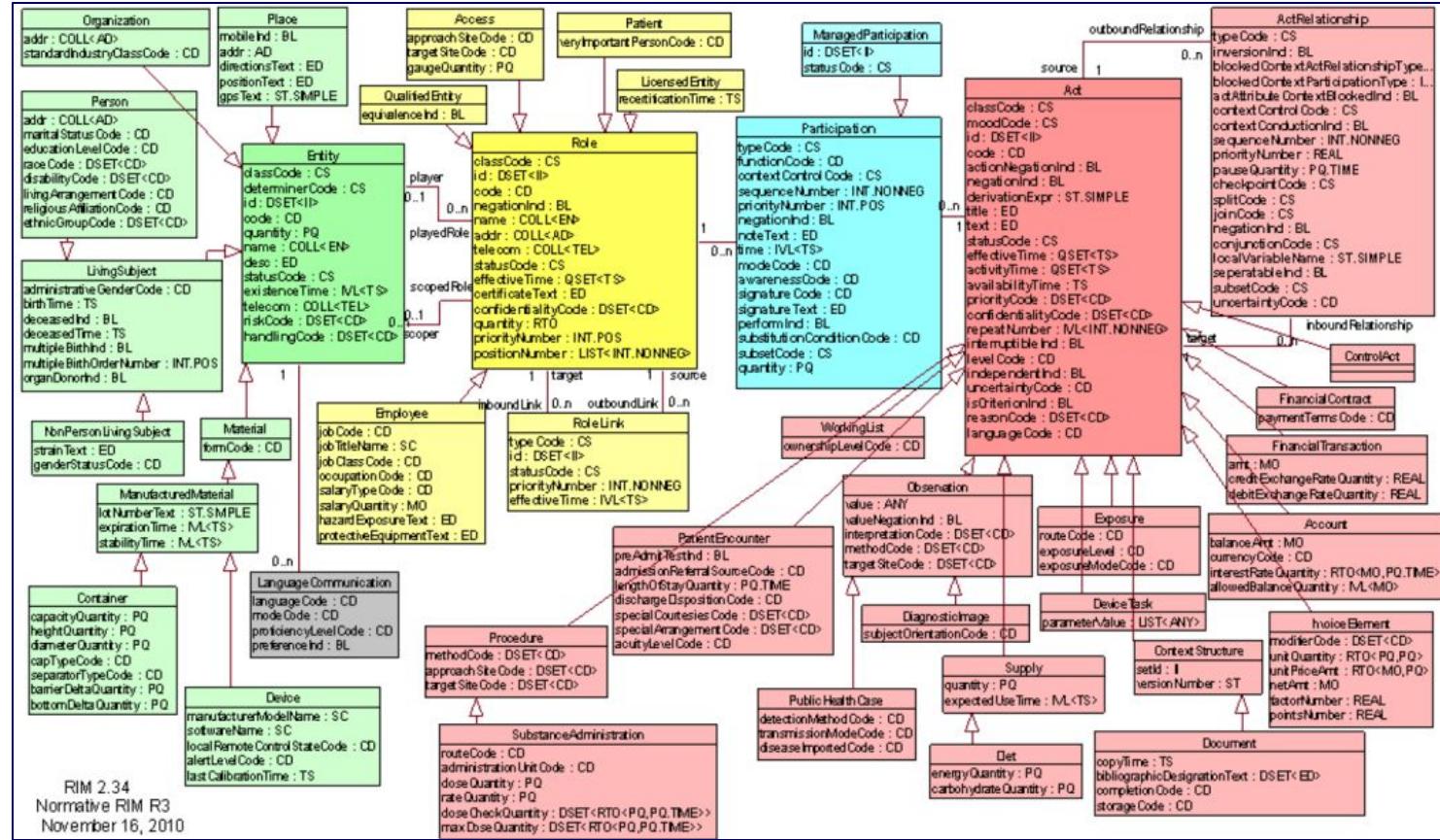


UNIVERSIDAD CES
Un compromiso con la excelencia

HL7 Ver.3 CDA

CDA (Clinical Document Architecture) fue reconocida como estándar ANSI en Noviembre del 2000 propone una estructura de documentos en formato XML, que gracias al uso del RIM (Modelo de Información de Referencia de HL7) y vocabularios codificados, el CDA convierte a los documentos clínicos, en objetos interpretables por multitud de aplicaciones y transferibles a través de cualquier medio electrónico.





RIM 2.34

Normative RIM R3
November 16, 2010

HL7 v3: RIM



UNIVERSIDAD CES
Un compromiso con la excelencia

HL7 Ver.3 CDA Historia

En enero de 1997 se realiza la primera reunión del Special Interest Group de HL7 dedicado al Standard Generalized Markup Language. En septiembre de 1998 se presenta el antecesor de CDA, Patient Record Architecture. En septiembre de 2000 se vota, como estándar HL7, el CDA R1.0 (release 1.0). En noviembre de 2000 se declara a CDA R1.0 como estándar ANSI.

En julio de 2003 se vota el primer ballot de CDA R2. En enero de 2005 se vota a CDA R2 como estándar HL7. En abril de 2005 se declara a CDA R2 como estándar ANSI.



UNIVERSIDAD CES
Un compromiso con la excelencia

HL7 Ver.3 CDA Características

- **Persistencia** : un documento clínico continúa existiendo sin alteraciones por un tiempo definido por requerimientos locales y regulatorios.
- **Responsabilidad** : un documento clínico debe ser mantenido por una organización a la que se asigna su cuidado.
- **Potencial para autenticación** : un documento clínico es un paquete de información que tiene prevista su autenticación legal.
- **Contexto** : un documento clínico establece un contexto para su contenido (paciente, prestador, participantes, etcétera).
- **Completitud** : la autenticación o firma de un documento clínico aplica a todo su contenido y no a porciones del contenido sin el contexto del documento.
- **Legibilidad** : el documento debe ser leído sin inconvenientes por los seres humanos.



UNIVERSIDAD CES
Un compromiso con la excelencia

HL7 Ver.3 CDA Alcance

- **El RIM, y no CDA**, define el contenido clínico de los documentos. El CDA estandariza exclusivamente la estructura y la semántica necesaria para el intercambio de documentos.
- **Mensajería** : la especificación de mensajes para el uso de CDA está fuera de su especificación; esta sugiere cómo empaquetar un documento CDA dentro de un mensaje HL7 v2.x y v3.
- **Administración** : CDA no especifica la creación o el manejo de documentos, sino sólo su marcación. La administración de documentos es interdependiente con CDA, pero la especificación de mensajes para la administración de documentos está fuera del alcance.



HL7 Ver.3 CDA Alcance: Escenarios de comunicación a través de documentos CDA

- **Comunicación entre prestadores y financiadores:** con fines de auditoría e historia clínica del afiliado/beneficiario.
- **Comunicación entre prestadores:** historia clínica del paciente (derivación, cambio, interconsulta) e informes médicos.
- **Comunicación entre financiadores:** historia clínica (cambio de financiador, cobertura compartida).
- **Comunicación entre prestadores/financiadores y salud pública:** historia clínica universal, historia clínica de pacientes de riesgo.
- **Comunicación entre salud pública y prestadores/financiadores:** historia clínica universal.



HL7 Ver.3 CDA Objetivos

- Dar prioridad a la atención del paciente.
- Permitir una implementación rentable que abarque el más amplio espectro de sistemas que sea posible.
- Soportar el intercambio de documentos entre usuarios de diferentes niveles de desarrollo tecnológico.
- Promover la longevidad de toda la información basada en esta arquitectura.
- Habilitar un amplio rango de aplicaciones de procesos post-intercambio.
- Promover un intercambio independiente de la transferencia o del mecanismo de almacenamiento.
- Preparar el diseño razonablemente rápido.
- Habilitar a los reguladores a controlar sus propios requerimientos de información sin tener que extender esta especificación.

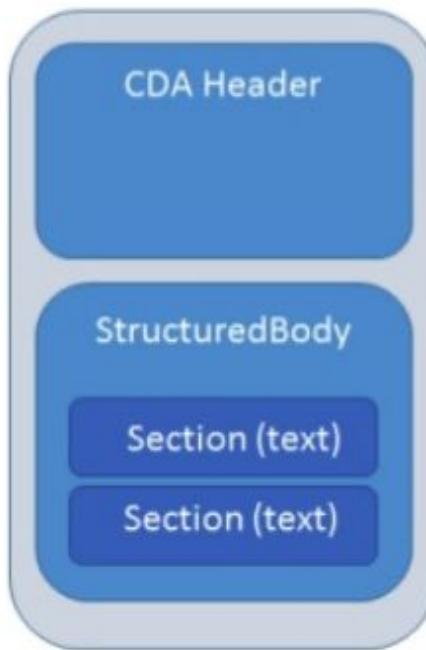


UNIVERSIDAD CES
Un compromiso con la excelencia

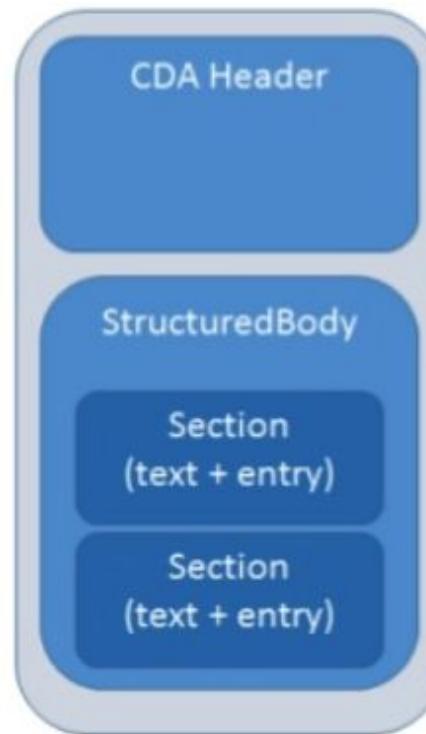
CDA level 1



CDA level 2



CDA level 3

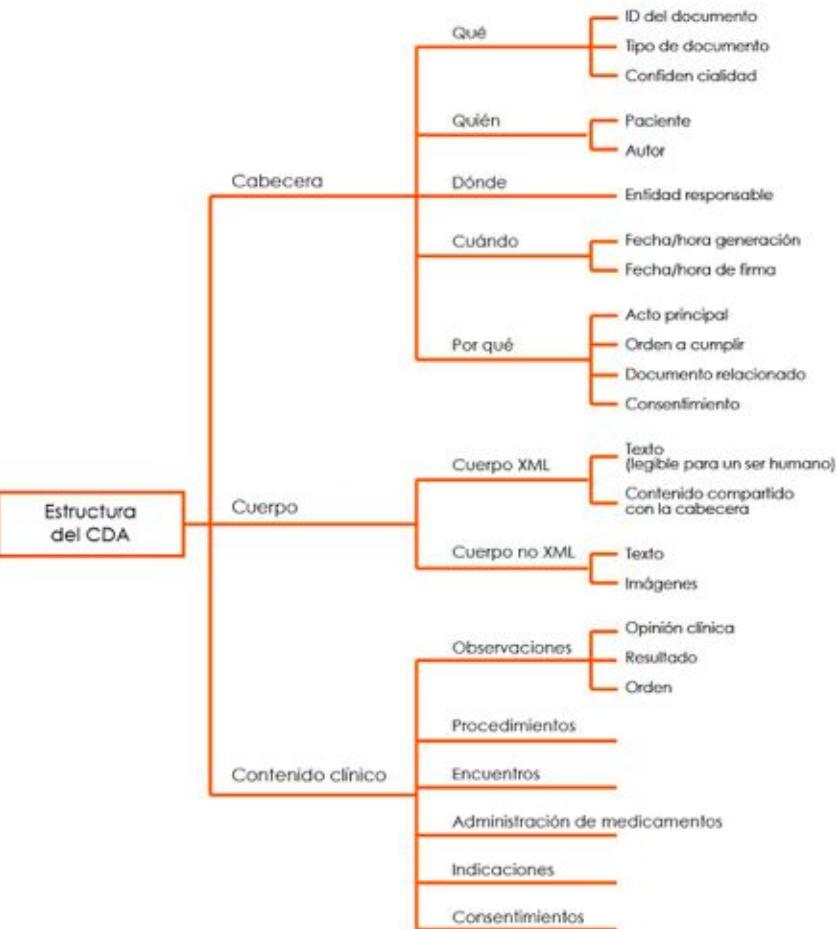


CDA Estructura



UNIVERSIDAD CES
Un compromiso con la excelencia

CDA Estructura



CDA Estructura

```
<ClinicalDocument xmlns="urn:hl7-org:v3" classCode="DOCCLIN" moodCode="EVN">
    <!-- **** ENCABEZADO DEL DOCUMENTO ELECTRÓNICO - HL7 CDA R2
        **** -->
    <typeId root="2.16.840.1.113883.1.3" extension="POCD_HD000040"/>
    <!-- Atributos del encabezado -->
    ...
    <!-- Participaciones del encabezado -->
    <recordTarget typeCode="RCT"></recordTarget>
    <author typeCode="AUT"></author>
    <dataEnterer typeCode="ENT"></dataEnterer>
    <informant typeCode="INF"></informant>
    <custodian typeCode="CST"></custodian>
    <informationRecipient typeCode="PRCP"></informationRecipient>
    <legalAuthenticator typeCode="LA"></legalAuthenticator>
    <authenticator typeCode="AUTHEN"></authenticator>
    <participant></participant>
    ...
    <component typeCode="COMP" contextConductionInd="true">
        <!-- **** CUERPO DEL DOCUMENTO ELECTRÓNICO - HL7 CDA R2
            **** -->
        </component>
    </ClinicalDocument>
```



Hospital Italiano - Consulta Ambulatoria



HOSPITAL
ITALIANO
de Buenos Aires

Paciente: MARIA CRISTINA MOYANO

Nro. HC: 42776

Fecha de Nacimiento: 25 de Febrero de 1977

Sexo: Femenino

Profesional: DANIEL ROBERTO LUNA

Creado el: 15 de Diciembre de 2005

PROBLEMAS (Nuevos)

- LUMBALGIA (Activo)

EVOLUCIONES (Ambulatorias)

- LUMBALGIA (Activo) - Tto sintomatico, sin irradiacion ni foco neurologico.

INDICACIONES FARMACOLOGICAS

PRODUCTO	CANTIDAD CRONICO TRAT_PROLONGADO
DIOXAFLLEX B12 Iny. Amp. x 6 1	0 N

Firmado por: DANIEL ROBERTO LUNA . fecha: 15 de Diciembre de 2005

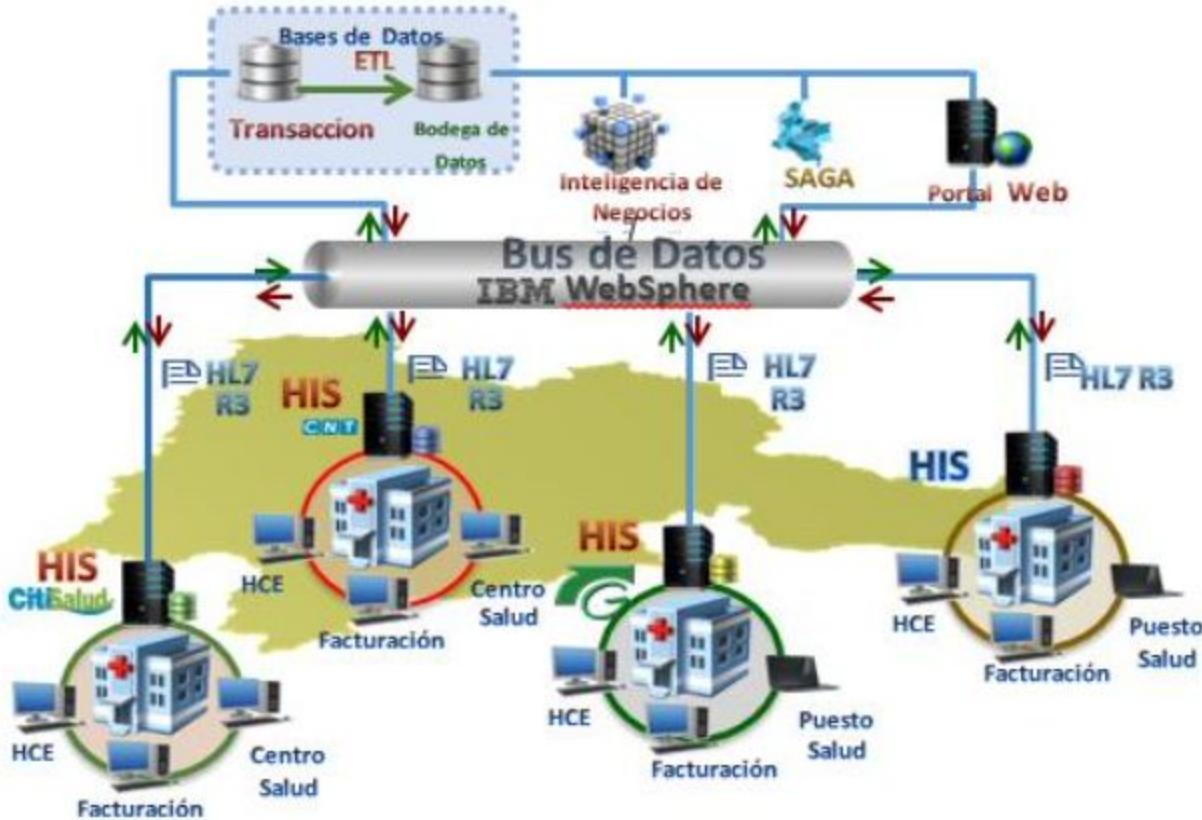


CCD.xml

https://docs.google.com/document/d/1ka_QDowTPw0KJYNlww0Idylc0I-oZ9UjMYmoSfYC3QM/edit?usp=sharing



UNIVERSIDAD CES
Un compromiso con la excelencia



Tomado del documento del manual del SIUS – Secretaría de Salud de Cundinamarca



La Historia Clínica Compartida en Catalunya y la Carpeta Personal de Salud



El modelo sanitario catalán

El sistema sanitario catalán

- La historia del Sistema Sanitario Catalán ha provocado que sea altamente fragmentado
 - Cerca del 80% de los proveedores de atención especializada y el 20% de atención primaria son entidades que no pertenecen al Departamento de Salud
 - Las farmacias operan de forma independiente
 - Existen colegios de profesionales con un importante peso de decisión



El Departamento de Salud está promoviendo soluciones TIC que integren los sistemas fragmentados



El modelo sanitario catalán

El sistema sanitario catalán

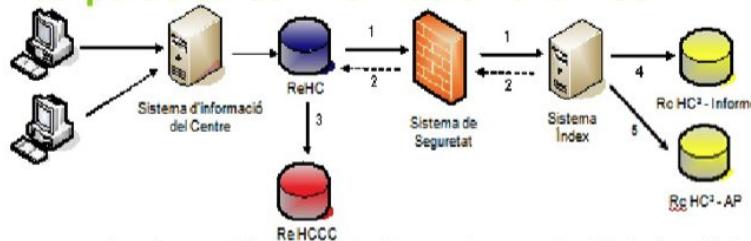


Interoperabilidad y estándares como elementos para maximizar la integración entre niveles asistenciales y diferentes proveedores del sistema

La Historia Clínica Compartida en Catalunya

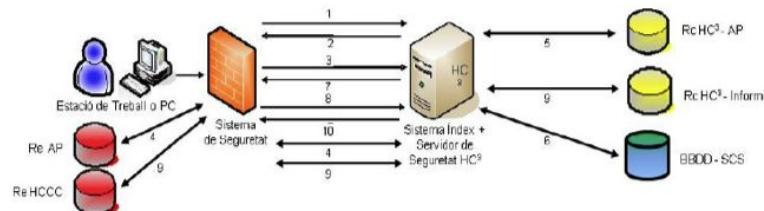
Proceso de publicación de información y acceso a la información

✓ Proceso de incorporación de información a la HC3



- El médico o enfermera, desde su sitio de trabajo, enriquece la historia clínica (HC) del paciente. El sistema de información del centro o entidad (SIC) lo va guardando automáticamente en el repositorio de la HC de la entidad o centro (ReHC). A continuación, para pasar la información de la HC de centro a la HC compartida en Catalunya.

✓ Acceso a la información y contenidos de la HC³



- Los circuitos son similares en el acceso de profesionales asistenciales y de ciudadanos. El proceso varía según sean Mensajes de identificación (se debe aportar datos de control), Información al Visor que solicita información Documentos e informes (del repositorio central o del centro)

La Carpeta Personal de Salud

¿Qué información habrá en la Carpeta Personal de Salud?

- Un espacio digital que permita al ciudadano disponer y utilizar su información personal de salud, y donde accederá mediante un certificado digital(CATCert, DNI_e)
- Iniciativas de este tipo facilitan la actitud proactiva del ciudadano, que puede ejercer su responsabilidad en el cuidado de su salud



Objetivos HC3

Continuidad asistencial

- Favorecer la **continuidad asistencial** y contribuir a fomentar el cuidado de la propia salud

Eficiencia

- Disminuir la **duplicidad** de pruebas y mayor control de los tratamientos incompatibles

Soporte

- Aumentar el **soporte** a la actividad de los profesionales, a nivel asistencial y formativo

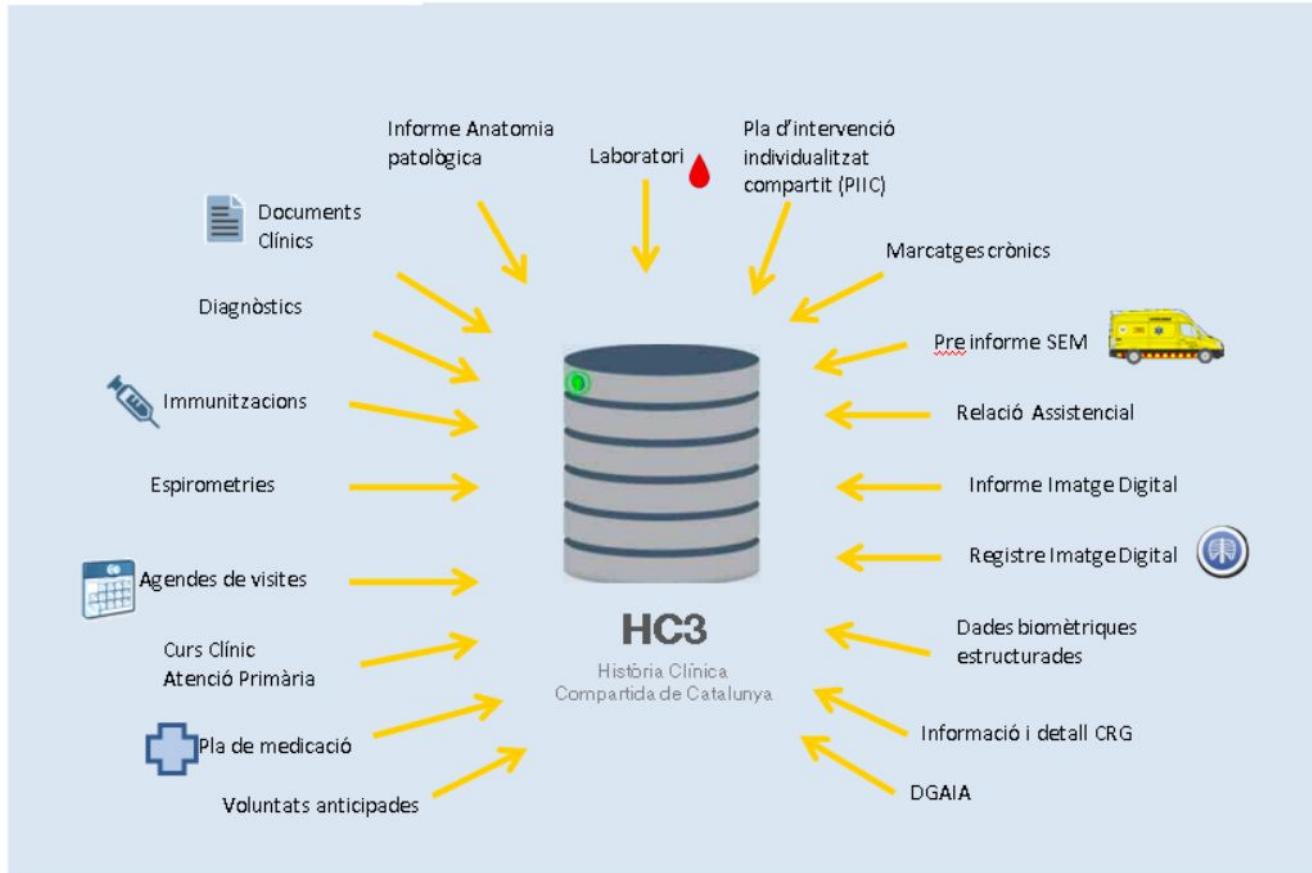
Seguridad de la información

- Generar más **confianza** de los pacientes en referencia a la seguridad de la información

Acceso a la información

- **Acceso a la información** y servicios más rápidos, flexibles y cómodos

HC3 Información disponible



Pacient: CIP ROE20620427014 - MIGNOLIA RO EZ - 46 Anys

[Ciutadà](#) [HC Resumida](#) [Documents](#) [Diagnòstics](#) [Farmàcia](#) [Immunitzacions](#) [Eines](#)

Ciutadà

[Manual](#)

Filiació

CIP: ROE20620427014 - MIGNOLIA RO EZ
Data de naixement: 27/04/1962 - 46 Anys Gènere: Home

DNI: 12345678Z N.A.S.S.: --

Contacte

Adreça: CR. MAJOR 109
Població de residència: MANRESA (08242)

Telèfon 1:
Telèfon 2:

Equip d'atenció primària

Metge atenció primària:
Infermera atenció primària:

Centre d'atenció domiciliària: AP PLAÇA DE CATALUNYA - MANRES...
Centre d'atenció primària: AP PLAÇA DE CATALUNYA - MANRES...

Avis legal

El projecte HCCC representa un gran avanç per a poder accedir a més informació relativa als pacients, però és necessari que tothom sigui conscient de la necessitat de preservar la confidencialitat de les dades accessible per mitjà de la HCCC.

I. Tots els accessos queden enregistrats i són monitoritzats per a evitar consultes no permeses. Així mateix aquesta informació d'accisos és utilitzada per a preservar la intimitat i confidencialitat de les dades dels pacients. Els pacients poden tenir coneixement del professionals que tenen accés a la seva història clínica per a poder exercir els drets que legalment ostenten.

II. L'ús de les dades i informació a la que vostè accedeixi per mitjà de la HCCC només podrà ser utilitzada per a les legítimes funcions del seu lloc de treball i sempre les haurà de tractar compliant amb les mesures de seguretat relatives a les dades de salut que formen part d'una història clínica.

Si vostè prem el botó "Accepto" manifesta que ha llegit el present avis legal, que el comprehé, que coneix els drets i deures en relació a l'accés a la HCCC establerts en el Conveni Tipus subscrit entre el Departament de Salut i els Centres, i que, per tant, legalment pot accedir a les dades que pretén consultar.

Jo ,

[Accepto](#) [Cancelar](#)



Ciutatà **HC Resumida** | [Documents](#) | [Diagnòstics](#) | [Farmàcia](#) | [Immunitzacions](#) | [Informacions altres CA](#) | [Consultes fetes](#)

HC Resumida

Manu

Prescripció Activa

Analítiques dels últims 6 mesos (0 informacions)

Informació d'AP i Especialitzada dels últims 12 mesos (0 informacions)

Informació internament i urgències dels últims 36 mesos (2 informacions)

12/12/2007 Informe mèdic ...	CENTRE D'ATE...	Genatri...
20/02/2006 Informe mèdic ...	HOSPITAL DEL...	Pneumolo...

Alertes i Problemes actius rellevants en AP (26 informacions)

ALERTES

29/12/2000 ANTECEDENTS PERSONALS D'AL-LÈRGIA A DROG...

PROBLEMES DE SALUT

14/02/2006 ALTERACIONS VISUALS, INESPECÍFIQUES

14/02/2006 RINITIS AL-LÈRGICA, NO ESPECIFICADA

31/10/2005 TUMOR BENIGNE DE LA GLÀNDULA SUPRARENAL

Condicionants de salut rellevants en AP

26/07/2000 DEPENDÈNCIA PER CONSUM DE TABA...

01/08/1960 DEPENDÈNCIA PER CONSUM D'ALCOH...

Procediments diagnòstics i terapèutics

31/01/2007 Perfusion corporal total HOSPITAL DELS ...

El Visor

Documentos

Generalitat de Catalunya
Departament de Salut

HC³ | Història Clínica Compartida a Catalunya

Pacient: CIP: ROEZ0620427014 - MIGNOLIA RO EZ - 46 Anys

Usuari: Maria Rovira
Manual | Desconnexió

Clitudà | HC Resumida | **Documents** | Diagnòstics | Farmàcia | Immunitzacions | Eines

Documents > Format Tabular

Ocultar/Mostrar Criteris de cerca Manual

S'ha trobat un total de 2 resultats. Mostrant del 1 al 2

Notif. Data Tipus d'informe Diagnòstic Servei Centre Assistencial Professional

<input type="checkbox"/>	20/02/2006	Informe mèdic a l'alta d'intemament	<input checked="" type="checkbox"/> Bronquitis no especificada com...	Pneumologia	HOSPITAL DELS PIRINEUS	
<input type="checkbox"/>	19/04/2004	Informe mèdic a l'alta d'intemament	<input checked="" type="checkbox"/> Ulcera duodenal aguda, remanent...	Aparell Digestiu	HOSPITAL DELS PIRINEUS	

Opció: Notificar

https://pre.hccc.salut.gencat.net/hccc/AppJava/getdocuments.wd?reqCode=get&clientCodePubFile=70 - Microsoft Internet Explorer p

Hospital dels Pirineus

CIP: ROEZ0620427014

Informe d'assistència

Pacient de 72 anys d'edat que ingressa en el Servei de Pneumologia procedent d'Urgències per augment de la seva disnea habitual.

The screenshot shows a web-based medical record system for Catalonia. At the top, there's a header with the logo of the Generalitat de Catalunya, the Department of Health, and the HC³ logo. Below the header, a navigation bar includes links for Clitudà, HC Resumida, Documents, Diagnòstics, Farmàcia, Immunitzacions, and Eines. The 'Documents' link is highlighted in red. A sub-menu for 'Format Tabular' is open. The main content area displays a table of medical records with columns for Notif., Data, Tipus d'informe, Diagnòstic, Servei, Centre Assistencial, and Professional. Two rows of data are shown, each with a checkbox in the Notif. column and a date in the Data column. The Diagnòstic column contains two entries, both preceded by a red circle and a red arrow pointing to it. Below the table, there's an 'Opció: Notificar' button. To the right, a separate window titled 'Microsoft Internet Explorer p' shows a PDF document from 'HOSPITAL DELS PIRINEUS' with the CIP number 'ROEZ0620427014'. The PDF page has a title 'Informe d'assistència' and a text section about a patient with respiratory distress. The bottom left corner of the slide contains the URL 'www.ces.edu.co'.

Pacient: CIP ROE20620427014 - MIGNOLIA RO EZ - 46 Anys

[Ciutadà](#) [HC Resumida](#) [Documents](#) [Diagnòstics](#) [Farmàcia](#) [Immunitzacions](#) [Eines](#)

Farmàcia > Prescripció - format tabular

[Ocultar](#)/[Mostrar](#) Criteris de Cerca [Manual](#)

S'ha trobat un total de 2 resultats. Mostrant del 1 al 2

[Primer](#) [Anterior](#) [Següent](#) [Últim](#)

Medicació	Data	Dosi	Freqüència	Durada	Crònic	Centre prescriptor	Professional
RIFATER 100 COMPRIMIDOS RECUBIERTOS	21/09/2008	3 pastilla	Cada 8 horas	7 dies		AP PLAÇA DE CATALUNYA - MANRES...	
CALOGEN 100UI 10 AMPOLLAS 1ML	28/01/2008	1	Cada 8 horas	20 dies	S	AP PLAÇA DE CATALUNYA - MANRES...	

Pacient: CIP ROE20620427014 - MIGNOLIA RO EZ - 46 Anys

[Ciutadà](#) [HC Resumida](#) [Documents](#) [Diagnòstics](#) [Farmàcia](#) [Immunitzacions](#) [Eines](#)

Farmàcia > Prescripció - format gràfic

[Ocultar](#)/[Mostrar](#) Criteris de Cerca [Manual](#)

S'ha trobat un total de 2 resultats. Mostrant del 1 al 2

[Primer](#) [Anterior](#) [Següent](#) [Últim](#)

Medicació Prescrita	2008											
	12	11	10	09	08	07	06	05	04	03	02	01
<input checked="" type="checkbox"/> RIFATER 100 COMPRIMIDOS RECUBIERTOS				■								
<input checked="" type="checkbox"/> CALOGEN 100UI 10 AMPOLLAS 1ML											■	

El Visor

Inmunizaciones



HC³ | Història Clínica
Compartida a Catalunya

Usuari: Maria Rovira
[Manual](#) | [Desconnexió](#)

Pacient: CIP ROEZ0620427014 - MIGNOLIA RO EZ - 46 Anys

[Ciutadà](#) [HC Resumida](#) [Documents](#) [Diagnòstics](#) [Farmàcia](#) [Inmunitzacions](#) [Eines](#)

[Inmunitzacions](#) > Format Tabular

[Manual](#)

S'ha trobat un total de 12 resultats. Mostrant del 1 al 12

[Primer](#) [Anterior](#) [Següent](#) [Últim](#)

Vacuna	1a dosi	2a dosi	3a dosi	4a dosi
Tétanos	29/04/1976	29/05/1976	29/04/1977	29/04/1997 
Difteria	29/04/1977			
Grip	29/04/1997			
Poliomielitis	29/04/1997			
Parotiditis	04/07/1997			
Rubéola	04/07/1997			
Varicella	04/07/1997			
Xarampió	04/07/1997			
Hepatitis A	20/09/1999	20/11/1999		
Hepatitis B	20/09/1999	20/11/1999		
	1a dosi			

Pacient: CIP ROEZ0620427014 - MIGNOLIA RO EZ - 46 Anys

[Ciutadà](#) [HC Resumida](#) [Documents](#) [Diagnòstics](#) [Farmàcia](#) [Immunitzacions](#) [Eines](#)

Personalització > Documents

[Manual](#)

Documents

Nombre de mesos a visualitzar:

Tipus informe(s):

Tots

Altres procediments D-T intervencionistes
Atenció especialitzada
Atenció especialitzada ambulatoria alta
Atenció especialitzada ambulatoria mitjana

Grup(s) de Diagnòstics CIM-9-CM:

Tots
Afeccions Originades en el Període Perinatal
Anomalies Congènites
Complicacions d' Embaràs, Part i Puerperi
Lesions i Emmetritisaments

Grup(s) de Diagnòstics CIN-10:

Tots
Causes externes de morbilitat i mortalitat
Certes afeccions originades en el període perinatal
Embaràs, part i puerperi
Factors que influïxen en l'estat de salut i contacte amb els serveis

Grup(s) de Diagnòstics CIAF-2:

Tots
Aparat circulatori
Aparat digestiu
Aparat ginecològic femení (inclou mama)
Aparat ginecològic masculí

Grup(s) de Diagnòstics NANDA:

Tots
Activitat/Repos
Afrontament/tolerància a l'estrés
Autopercepció
Curfuit

Autoregistro

- código de usuario y contraseña

Certificado Digital

- documento electrónico que permite garantizar la identidad de la persona que está consultando los datos

Visión PC y tableta

Generalitat de Catalunya
Departament de Salut

CatSalut

la meva
salut

Accés a Cat@Salut La Meva Salut

1. Introduïu el vostre CIP
CIP: _____

2. Identifiqueu-vos amb un dels sistemes d'autenticació

Paraula de pas Certificat digital

Com obtenir la paraula de pas
He oblidat la meva paraula de pas

3. Introduïu codi usuari / paraula pas
Codi d'usuari: _____
Paraula de pas: _____

Accedeix

NAAE 1 73217000 5
entrega mèdica en línia
consultes mèdiques en línia

Visión móvil

Generalitat de Catalunya
Departament de Salut

CatSalut

Benvinguts/des al Cat@Salut La Meva Salut

la meva
salut

Certificat digital Paraula de pas

Per accedir
Cat@Salut La Meva
Salut introduceix el seu
CIP:

Menú



Fast Healthcare Interoperability Resources (FHIR)



UNIVERSIDAD CES
Un compromiso con la excelencia

Por qué FHIR

- La versión 2 fue (y es) extremadamente exitosa, pero la tecnología es antigua y no muy adecuada para los requerimientos más recientes.
- La versión 3, aunque se basa en un modelo sólido, no ha sido ampliamente aceptada y es percibida como difícil de implementar.
- El CDA ha sido enormemente exitoso, pero fue diseñado como un documento y al usarlo de otra manera realmente no encaja bien en todos los escenarios.
- Las herramientas para los estándares de HL7 siempre han sido un problema, ya que por lo general deben ser diseñadas y construidas—específicamente para HL7 y esto no siempre sucede en los tiempos adecuados.
- hay nuevos casos de uso especialmente los que involucran dispositivos móviles, donde los estándares actuales no encajan bien;
- Particularmente en el ámbito online, la arquitectura basada en representational state transfer (REST, transferencia de estado representativo) se usa ampliamente en otros dominios.



UNIVERSIDAD CES
Un compromiso con la excelencia

Por qué FHIR

FHIR es la abreviatura de Fast Healthcare Interoperability Resources, es decir, recursos de interoperabilidad rápida en salud. Se desarrolla a partir del trabajo mencionado. El objetivo de FHIR es producir un estándar.

- Que sea fácil de desarrollar con una curva baja de aprendizaje y con requerimientos mínimos de herramientas específicas.
- Que sea fácil de implementar (o tan fácil como puede serlo la interoperabilidad en salud).
- Que sea semánticamente sólido, esto significa que pueda ser mapeado con el RIM v 3 (y, a menudo, con otras especificaciones, como los arquetipos de openEHR);
- Que sea “amigable” para el implementador; por ejemplo, que utilice herramientas y formatos comunes y tecnologías basadas en web para la especificación;
- Cuyos artefactos tengan sentido para la vista humana. Aunque no están destinados a ser vistos directamente por un ser humano, que sean entendibles ayuda tanto a los implementadores como al personal de soporte;
- Cuyos artefactos puedan ser validados electrónicamente (tanto como sea posible);
- Que se integre bien y promueva las tecnologías modernas de comunicación basadas en web (HTTP, XML, JSON, etcétera).



FHIR : Alcance (contenido, infraestructura, uso)

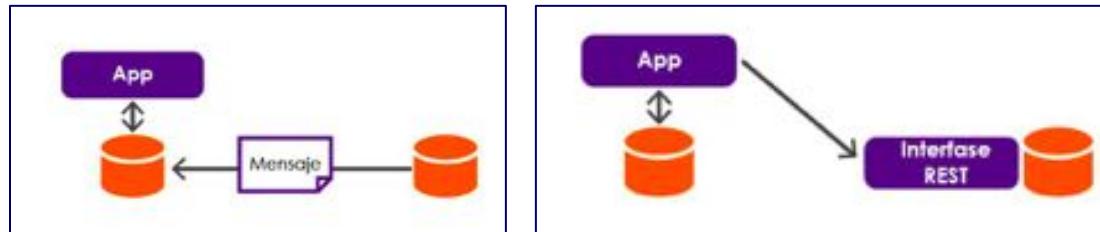
El alcance de FHIR incluye todos los aspectos de la interoperabilidad relacionada con la salud-atención clínica, la administración, la investigación, etc. Además, FHIR soporta la interoperabilidad mediante cuatro arquitecturas o paradigmas de intercambio de información. Estos son:

1. Mensajería.
2. Documentos.
3. Servicios REST.
4. Acceso en línea.

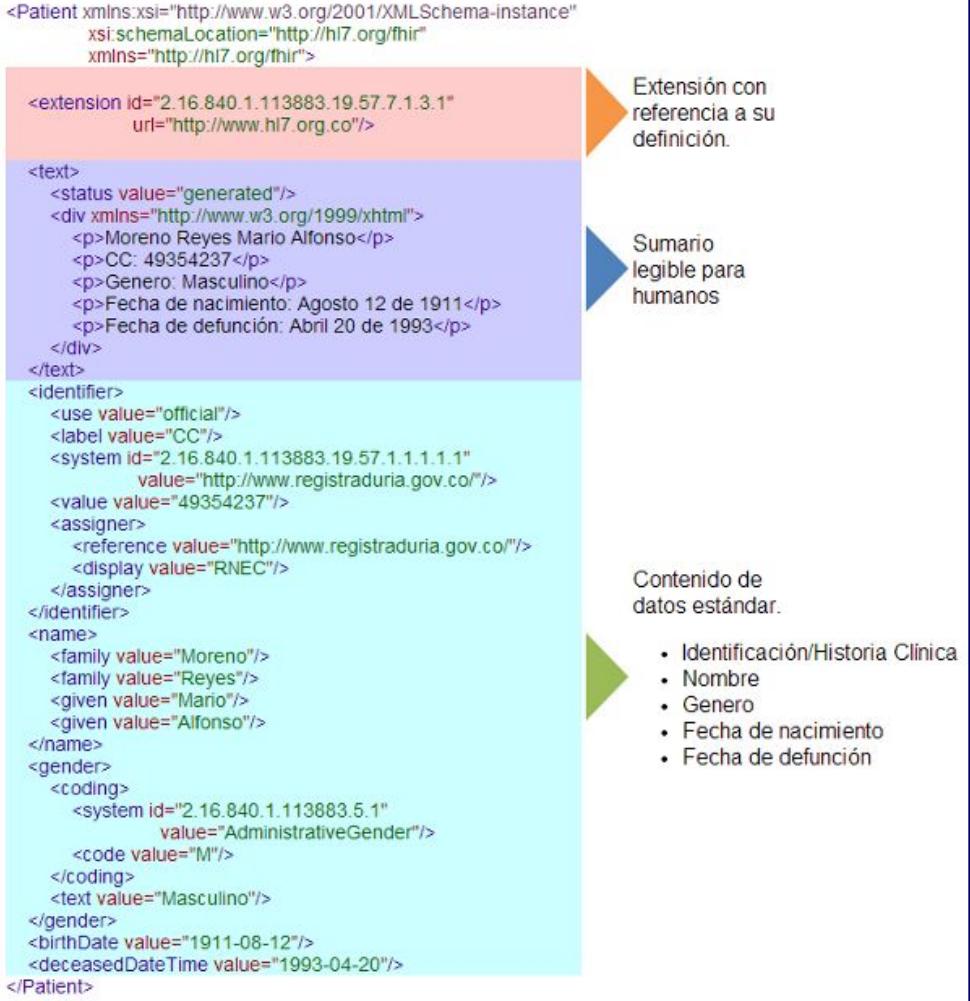


FHIR : Alcance (contenido, infraestructura, uso)

HL7 tiene considerable experiencia con los paradigmas de mensajería y documentos, y alguna experiencia en el paradigma de servicios. Sin embargo, REST es nuevo para HL7. A diferencia del paradigma de mensajería, donde los mensajes se usan para actualizar repositorios (así como para implementar conductas), el paradigma REST posibilita que se acceda a la información desde otro servidor cuando sea necesario, por lo que, más bien, soporta un modelo distribuido.



FHIR :
ejemplo de un **recurso** tipo "paciente", que contiene la información de identificación básica y datos demográficos del paciente:



Representación de FHIR® empleando JSON - Ejemplo 1

```
{  
    "resourceType": "Patient",  
    "text": {  
        "status": "generated",  
        "div": "<div xmlns="http://www.w3.org/1999/xhtml">  
            <p>Moreno Reyes Mario Alfonso</p>  
            <p>CC: 49354237</p>  
            <p>Genero: Masculino</p>  
            <p>Fecha de nacimiento: Agosto 12 de 1911</p>  
            <p>Fecha de defunción: Abril 20 de 1993</p>  
        </div><br>",  
        "identifier": [  
            {"use": "official",  
             "label": "CC",  
             "system": "http://www.registraduria.gov.co/",  
             "value": "49354237",  
             "assigner": {"reference": "http://www.registraduria.gov.co/",  
                         "display": "RNEC"}],  
            "name": [  
                {"family": ["Moreno", "Reyes"],  
                 "given": ["Mario", "Alfonso"]}],  
            "gender": {  
                "coding": [  
                    {"system": "AdministrativeGender",  
                     "code": "M"}],  
                "text": "Masculino"},  
                "birthDate": "1911-08-12",  
                "deceasedDateTime": "1993-04-20",  
            }  
    }  
}
```

*Nota:

El contenido XHTML en el elemento 'div' que se encuentra en el elemento narrativo 'text' se representa como una cadena literal en el valor de propiedad en JSON.
La cadena ha sido alterada para que pueda visualizarse en el ejemplo
(es necesario eliminar los saltos de línea).

REST (Transferencia de Estado Representacional)

FHIR trabaja con diferentes paradigmas de interoperabilidad, pero REST, a esta altura, está establecido, por lejos, como el de uso más fácil, y demostramos por qué. Actualmente, lo usan compañías como Google, Amazon y Twitter para proveer acceso a sus servicios. A pesar de lo complicado de su nombre, en realidad es verdaderamente simple; de hecho, es cómo funciona la web hoy.

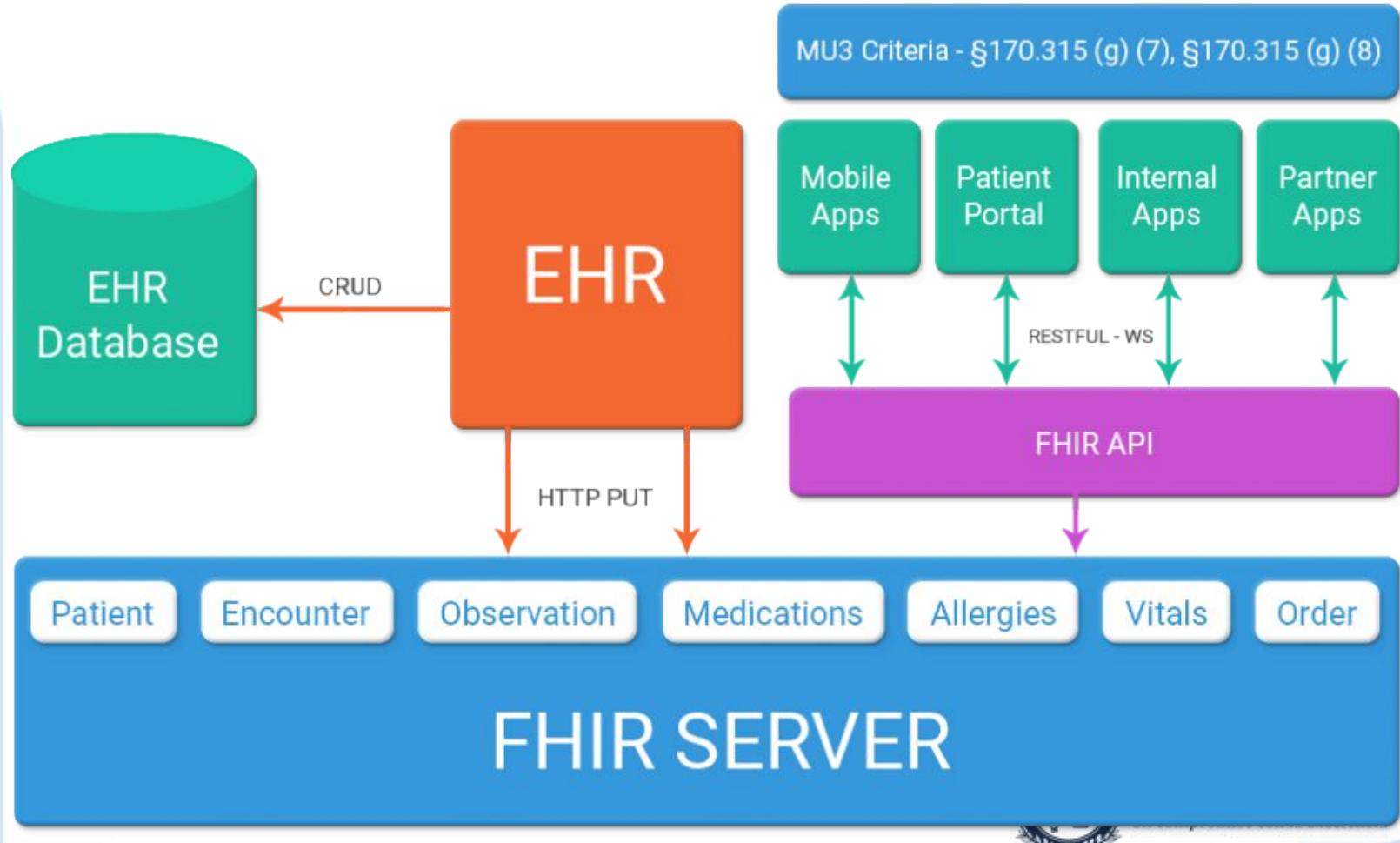


REST

Cuando trabajamos con recursos, hay un número fijo de métodos a ejecutar. Los que realmente nos interesan en FHIR son:

- **GET** . Es para recuperar un recurso en particular basado en su identificador (en la ubicación en el servidor y el ID). FHIR usa GET tanto para traer un único recurso como para ejecutar consultas al servidor, que posiblemente retorne con muchos recursos.
- **POST** . Este método se usa para crear recursos nuevos en un servidor específico. En REST, el servidor asigna un ID y esa combinación se transforma en el identificador único para ese recurso.
- **PUT** . Este método actualiza un recurso ya existente. El cliente que ejecuta esta operación necesita saber el identificador del recurso. En FHIR, crea una versión nueva del recurso.
- **DELETE** . Este método borra un recurso. Otra vez, necesitamos saber cuál es su identificador único. FHIR recomienda guardar una copia de este recurso en el servidor, que puede ubicarse de alguna forma para acceder. De todas formas, si se ejecuta directamente un GET de ese recurso, no deberían retornar los que fueron borrados.
- **OPTIONS** . Este es un método “especial” en FHIR, dirigido a la raíz del servidor. Devuelve el conformance de cada recurso, es decir, cuáles son las capacidades que tiene el servidor.







<https://h5p.org/node/1111633>



UNIVERSIDAD CES
Un compromiso con la excelencia



Laboratorio HL7 FHIR 2,5%



UNIVERSIDAD CES
Un compromiso con la excelencia



The screenshot shows the FHIR.drawio application interface. The left sidebar contains toolbars for 'General' (with various shapes like rectangles, circles, arrows), 'Miscelánea' (with icons for lists, tables, etc.), 'Avanzado' (with icons for advanced shapes), 'Básico' (with icons for basic shapes), 'Flechas' (with icons for arrows), 'Diagrama de flujo' (with icons for flowcharts), 'Relación de la entidad' (with icons for entity relationships), and '+ Más formas...' (with a plus icon). The main workspace displays a logo for 'UNIVERSIDAD CES' and the text 'INGENIERÍA BIOMÉDICA', 'INTEROPERABILIDAD EN SALUD', and 'RECURSOS FHIR'. Below this, there is a section titled 'RECURSO JSON PARA SER ENVIADO POR FHIR' containing a JSON code block:

```
{
  "resourceType": "Observation",
  "id": "51",
  "meta": {
    "versionID": "1",
    "lastUpdated": "2018-08-20T03: 35:55.665-03:00"
  },
  "text": {
    "status": "generated",
    "div": "<div xmlns='http://www.w3.org/1999/xhtml'><test>",
    "status": "final",
    "code": {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "718-7",
          "display": "haemoglobin"
        }
      ],
      "subject": {
        "reference": "Patient/39"
      },
      "valueQuantity": {
        "value": 100,
        "unit": "g/L",
        "system": "http://unitsofmeasure.org",
        "code": "g/L"
      }
    }
  }
}
```

Below the JSON is a table titled 'MENSAJE EN JSON POR FHIR' with columns 'PREGUNTA' and 'RESPUESTA'. The rows are:

PREGUNTA	RESPUESTA
TIPO DE RECURSO	Text
TIPO DE CODIFICACIÓN	Text
CÓDIGO DEL RESULTADO	Text
NOMBRE DEL EXAMEN	Text
IDENTIFICACION DEL PACIENTE	Text
VALOR DEL RESULTADO	Text
UNIDAD DE MEDIDA	Text
VALORES DE REFERENCIA	Text

At the bottom, a pink box contains the text: 'PASO 1 - INSTRUCCIONES: Observe con detenimiento el recurso JSON que va a ser enviado por REST y diligencie los campos de texto con las respuestas correctas.'

The right sidebar includes sections for 'Diagrama' (with 'Vista' options like 'Cuadrícula' and 'Vista de la página'), 'Estilo' (with 'Fondo' and 'Sombra' options), 'Opciones' (with 'Flechas de conexión', 'Puntos de conexión', 'Guías', and 'Guardar automático' checked), 'Tamaño del papel' (set to 'US-Legal (8.5" x 14")' with 'Orientación vertical' selected), and buttons for 'Editar datos...' and 'Quitar estilo predeterminado'.

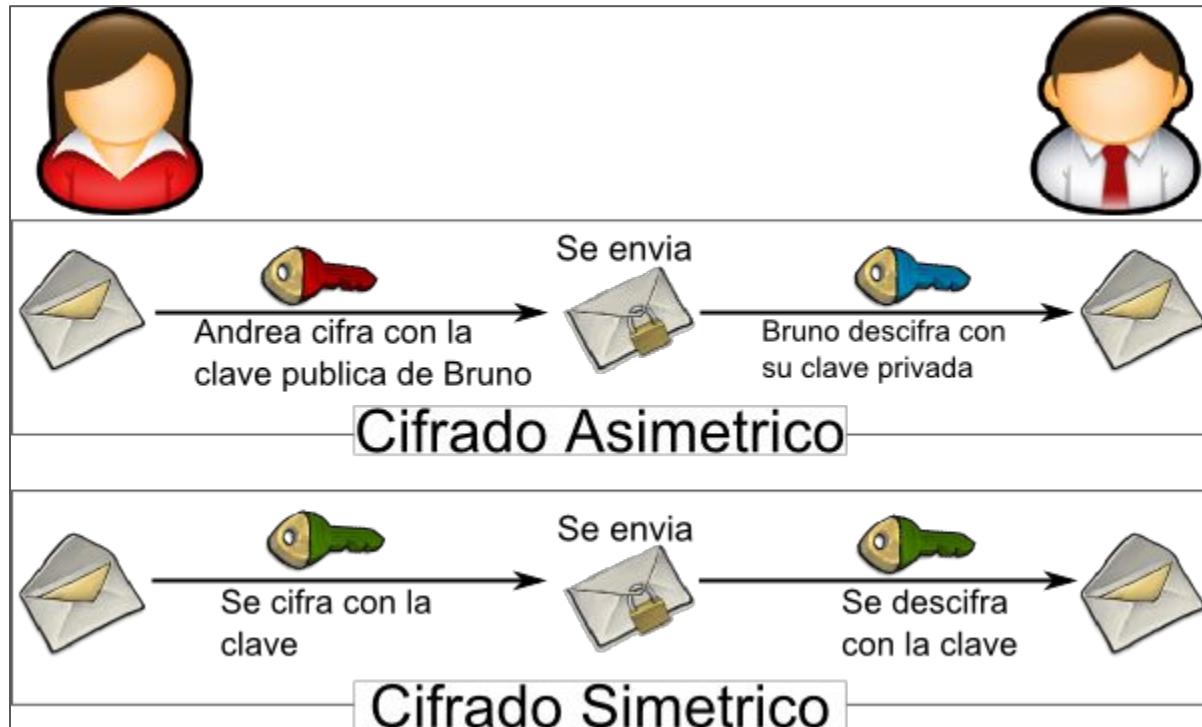


Seguridad de la información



UNIVERSIDAD CES
Un compromiso con la excelencia

Criptografía





En criptografía, **RSA (Rivest, Shamir y Adleman)** es un sistema criptográfico de clave pública desarrollado en 1979, que utiliza la factorización de números enteros. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

La seguridad de este algoritmo radica en el problema de la factorización de números enteros. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto. Actualmente estos primos son del orden de 10^{300} , y se prevé que su tamaño siempre crezca con el aumento de la capacidad de cálculo de los ordenadores.



UNIVERSIDAD CES
Un compromiso con la excelencia



Como en todo sistema de clave pública, cada usuario posee dos claves de cifrado: una pública y otra privada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada.

Se cree que RSA será seguro mientras no se conozcan formas rápidas de descomponer un número grande en producto de primos. Aunque se cree que la computación cuántica podría proveer de una solución al problema de factorización, existen investigadores que dudan que dichos avances vayan a volver obsoletos estos algoritmos.



UNIVERSIDAD CES
Un compromiso con la excelencia

Ejercicio Propuesto

RSA

Rivest, Shamir y Adleman

Ejemplo de cifrado de mensaje: *Ana envía un mensaje a David*

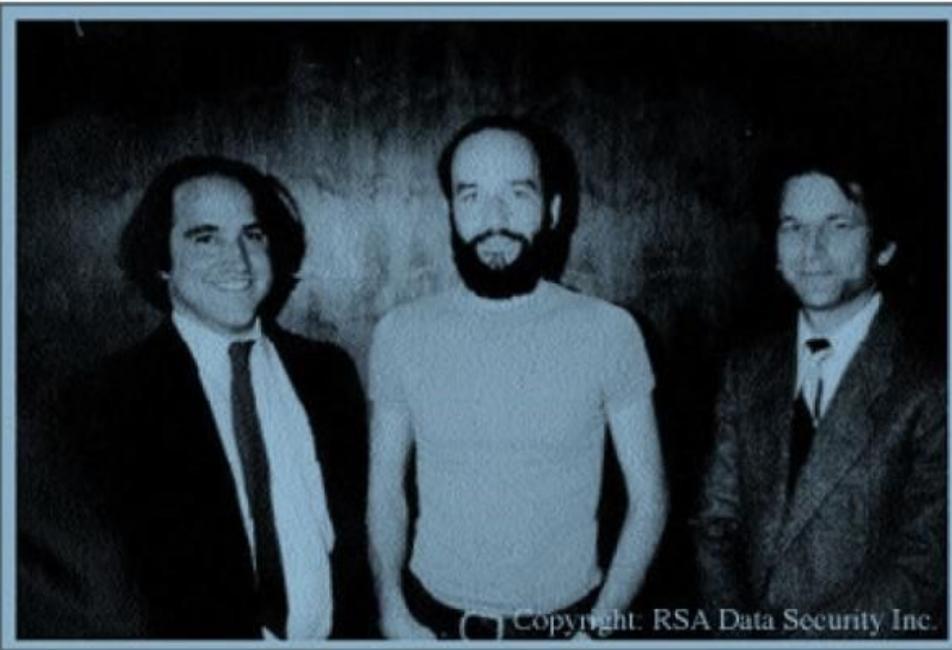


1. Ana redacta un mensaje.
2. Ana cifra el mensaje con la **clave pública** de David.
3. Ana envía el mensaje cifrado a David a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio.
4. David recibe el mensaje cifrado y lo descifra con su **clave privada**.
5. David ya puede leer el mensaje original que le mandó Ana.

Ejemplo de firma digital con clave asimétrica: *David envía un mensaje a Ana*



1. David redacta un mensaje.
2. David firma digitalmente el mensaje con su **clave privada**.
3. David envía el mensaje firmado digitalmente a Ana a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio.
4. Ana recibe el mensaje firmado digitalmente y comprueba su autenticidad usando la **clave pública** de David.
5. Ana ya puede leer el mensaje con total seguridad de que ha sido David el remitente.



1979



Marin Mersenne

$$2^{74,207,281} - 1$$

23 Millones de Dígitos



EL PEQUEÑO TEOREMA DE FERMAT

$$a^p \equiv a \pmod{p}$$

RSA
Rivest, Shamir y
Adleman



UNIVERSIDAD CES
Un compromiso con la excelencia

RSA - Claves

- Se buscan dos primos los suficientemente grandes: **p** y **q**, con **p** diferente de **q**
- Estos número en la realidad tienen cientos de dígitos
- Para nuestro ejemplo, serán **p=11** y **q=3**

RSA
Rivest, Shamir y
Adleman



RSA - Claves

- A partir de estos número se obtiene :
 $n = p * q$
 $\theta = (p - 1) * (q - 1)$
- En nuestro ejemplo :
 $n= 11 * 3 = 33$
 $\theta = (10 * 2) = 20$

RSA
Rivest, Shamir y
Adleman



RSA - Claves

- Se busca un número impar 'e' tal que no tenga múltiplos comunes con θ
- Para esto se selecciona de forma aleatoria un entero 'e' tal que $1 < e < \theta$
 $MCD(\theta, e) = 1$
En nuestro ejemplo :
 $e = 3 \quad MCD(20, 3) = 1$



RSA - Claves

- Se calcula el exponente privado de RSA

$$d = \text{inv}(e, \vartheta)$$

$$d = \text{inv}(3, 20) = 7 \rightarrow 3 * 7 \bmod 20 = 1$$

RSA
Rivest, Shamir y
Adleman



RSA - Claves

- Clave Pública
 $(e,n) = (3, 33)$
- Clave Privada
 $(d,n) = (7, 33)$

RSA
Rivest, Shamir y
Adleman



Ejercicio Propuesto

RSA
Rivest, Shamir y
Adleman

RSA - Claves

- Cifrado

$$C = M^e \text{ mod } n$$

- Descifrado

$$C^d \text{ mod } n = M$$



UNIVERSIDAD CES
Un compromiso con la excelencia

Ejercicio Propuesto

CODIFICACIÓN

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

-	0	1	2	3	4	5	6	7	8	9
26	27	28	29	30	31	32	33	34	35	36

S	E	G	U	R	I	D	A	D
18	4	6	20	17	8	3	0	3

RSA
Rivest, Shamir y
Adleman



Ejercicio Propuesto

RSA

Rivest, Shamir y
Adleman

CLAVE DE CIFRADO PÚBLICA : (3, 33)	
M = 18 4 6 20 17 8 3 0 3	
CÁLCULO	RESULTADO
$18^3 \text{ MOD } 33$	24
$4^3 \text{ MOD } 33$	31
$6^3 \text{ MOD } 33$	18
$20^3 \text{ MOD } 33$	14
$17^3 \text{ MOD } 33$	29
$8^3 \text{ MOD } 33$	17
$3^3 \text{ MOD } 33$	27
$0^3 \text{ MOD } 33$	0
$3^3 \text{ MOD } 33$	27



Ejercicio Propuesto

RSA

Rivest, Shamir y
Adleman

CLAVE DE CIFRADO PÚBLICA : (7, 33)	
$C = 24 \ 31 \ 18 \ 14 \ 29 \ 17 \ 27 \ 0 \ 27$	
CÁLCULO	RESULTADO
$24 ^ 7 \text{ MOD } 33$	18
$31 ^ 7 \text{ MOD } 33$	4
$18 ^ 7 \text{ MOD } 33$	6
$14 ^ 7 \text{ MOD } 33$	20
$29 ^ 7 \text{ MOD } 33$	17
$17 ^ 7 \text{ MOD } 33$	8
$27 ^ 7 \text{ MOD } 33$	3
$0 ^ 7 \text{ MOD } 33$	0
$27 ^ 7 \text{ MOD } 33$	3

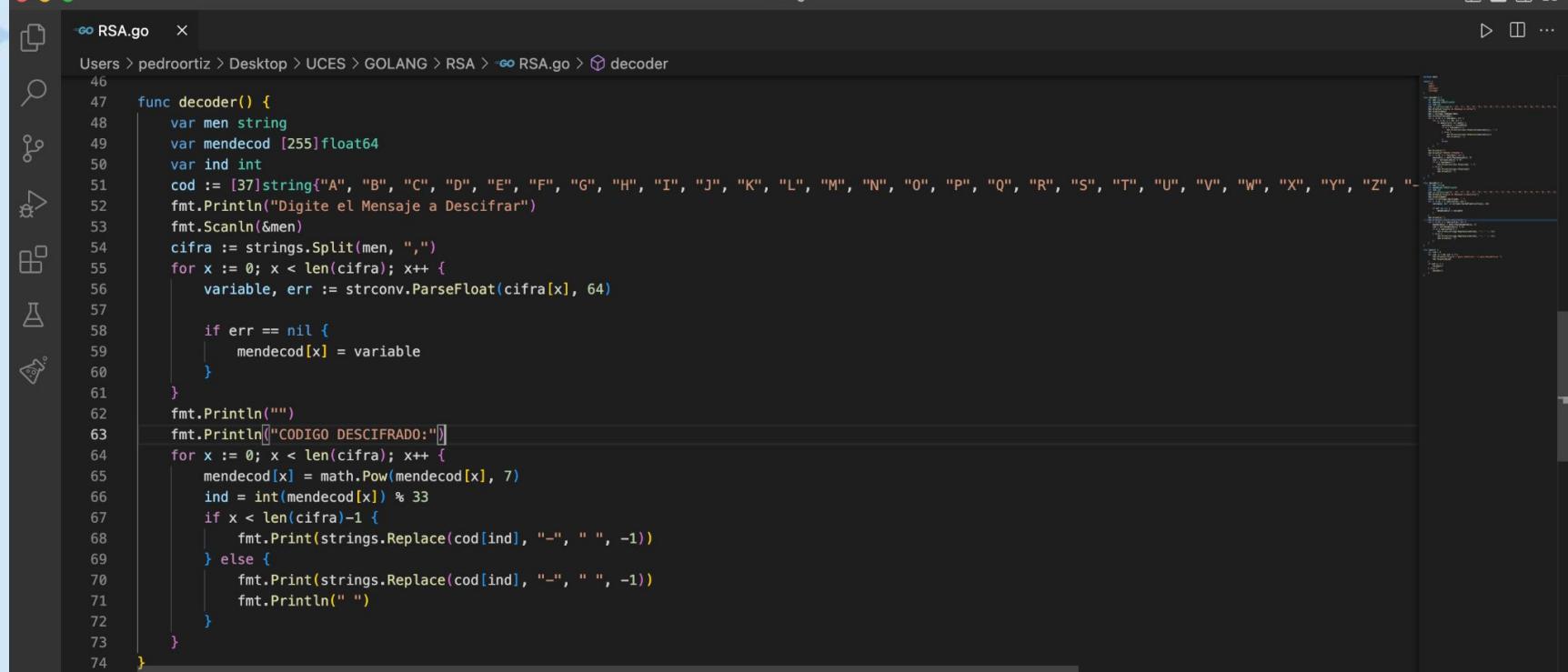


Ejercicio Propuesto

RSA
Rivest, Shamir y
Adleman

GRUPO	TEXTO CIFRADO
1	11,5,8,14,29,0,20,31,24,20,13,0,8,31,29,20,11,5,20,12,17,24,12,5,20,14,19,0,20,30,20,5,28,29,0,20,21,31,16,20,30,20,31,24,9,31,29,0,29,20,29,31,24,14,11,28,0,27,5,24,20,27,17,26,31,29,31,19,28,31,24,20,0,11,1,31,29,28,20,31,17,19,24,28,31,17,19
2	0,12,0,20,0,20,28,5,27,5,24,20,8,5,19,26,17,0,20,31,19,20,14,19,5,24,20,9,5,8,5,24,20,19,5,20,13,0,18,0,24,20,12,0,11,20,0,20,19,17,19,18,14,19,5,20,22,17,11,11,17,0,12,20,24,13,0,10,31,24,9,31,0,29,31
3	11,0,20,24,31,19,8,17,11,11,31,16,20,31,24,20,11,0,20,12,0,23,17,12,0,20,24,5,26,17,24,28,17,8,0,8,17,5,19,20,11,31,5,19,0,29,27,5,20,27,0,20,21,17,19,8,17
4	19,5,20,31,24,20,8,14,0,19,28,5,20,28,17,31,19,31,24,20,11,5,20,4,14,31,20,13,0,8,31,20,4,14,31,20,11,0,20,18,31,19,28,31,20,28,31,20,0,27,12,17,29,31,20,31,24,20,4,14,17,31,19,20,31,29,31,24,20,31,11,21,17,24,20,9,29,31,24,11,31,30
5	11,0,20,31,27,14,8,0,8,17,5,19,20,31,24,20,31,11,20,0,29,12,0,20,12,0,24,20,9,5,27,31,29,5,24,0,20,4,14,31,20,9,14,31,27,31,24,20,14,24,0,29,20,9,0,29,0,20,8,0,12,1,17,0,29,20,31,11,20,12,2,14,19,27,5,20,19,31,11,24,5,19,20,12,0,19,27,31,11,0
6	11,0,20,21,17,27,0,20,31,24,20,11,5,20,4,14,31,20,24,14,8,31,27,31,20,8,14,0,19,27,5,20,31,24,28,0,24,20,5,8,14,9,0,27,5,20,13,0,8,17,31,19,27,5,20,5,28,29,5,24,20,9,11,0,19,31,24,20,3,5,13,19,20,11,31,19,19,5,19
DOCENTE	31,11,20,24,31,18,14,19,27,5,20,31,24,20,31,11,20,9,29,17,12,31,29,5,20,27,31,20,11,5,24,20,9,31,29,27,31,27,5,29,31,24,20,0,30,29,28,5,19,20,24,31,19,19,0





```
func decoder() {
    var men string
    var mendecod [255]float64
    var ind int
    cod := [37]string{"A", "B", "C", "D", "E", "F", "G", "H", "I", "J", "K", "L", "M", "N", "O", "P", "Q", "R", "S", "T", "U", "V", "W", "X", "Y", "Z", "-"}
    fmt.Println("Digite el Mensaje a Descifrar")
    fmt.Scanln(&men)
    cifra := strings.Split(men, ",")
    for x := 0; x < len(cifra); x++ {
        variable, err := strconv.ParseFloat(cifra[x], 64)

        if err == nil {
            mendecod[x] = variable
        }
    }
    fmt.Println("")
    fmt.Println("CODIGO DESCIFRADO:")
    for x := 0; x < len(cifra); x++ {
        mendecod[x] = math.Pow(mendecod[x], 7)
        ind = int(mendecod[x]) % 33
        if x < len(cifra)-1 {
            fmt.Print(strings.Replace(cod[ind], "-", " ", -1))
        } else {
            fmt.Print(strings.Replace(cod[ind], "-", " ", -1))
            fmt.Println(" ")
        }
    }
}
```

PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE

zsh - RSA + ×

Digite 1 para Codificar / 2 para Decodificar

2

Digite el Mensaje a Descifrar

31,11,20,24,31,18,14,19,27,5,20,31,24,20,31,11,20,9,29,17,12,31,29,5,20,27,31,20,11,5,24,20,9,31,29,27,31,27,5,29,31,24,20,0,30,29,28,5,19,20,24,31,19,19,0

CODIGO DESCIFRADO:

EL SEGUNDO ES EL PRIMERO DE LOS PERDEDORES AYRTON SENNA

pedroortiz@MacBook-Air-de-PEDRO-3 RSA % go build RSA.go
pedroortiz@MacBook-Air-de-PEDRO-3 RSA %



RSA — -zsh — 80x24

```
[pedroortiz@MacBook-Air-de-PEDRO-3 RSA % ./RSA
```

```
Digite 1 para Codificar / 2 para Decodificar
```

```
2
```

```
Digite el Mensaje a Descifrar
```

```
31,11,20,24,31,18,14,19,27,5,20,31,24,20,31,11,20,9,29,17,12,31,29,5,20,27,31,20  
,11,5,24,20,9,31,29,27,31,27,5,29,31,24,20,0,30,29,28,5,19,20,24,31,19,19,0
```

CODIGO DESCIFRADO:

EL SEGUNDO ES EL PRIMERO DE LOS PERDEDORES AYRTON SENNA

```
pedroortiz@MacBook-Air-de-PEDRO-3 RSA %
```

FIN SESIÓN 4

¡Gracias!



UNIVERSIDAD CES
Un compromiso con la excelencia