BIG DATA WEEK
A GLOBAL FESTIVAL OF DATA

ReactoData

SEGURIDAD EN BIG DATA

IMPORTANCIA, QUE Y COMO

WHOAMI

Federico Leven

- @ ReactoData
- Big Data + Open Source desde 2012
- Coordinador Big Data Meetup (http://www.iaar.site), speaker ...
- federico@reactodata.net
- Web : http://www.reactodata.net/es
- Twitter: @reactodata
- Linkedin : https://www.linkedin.com/in/federicoleven/

ReactoData

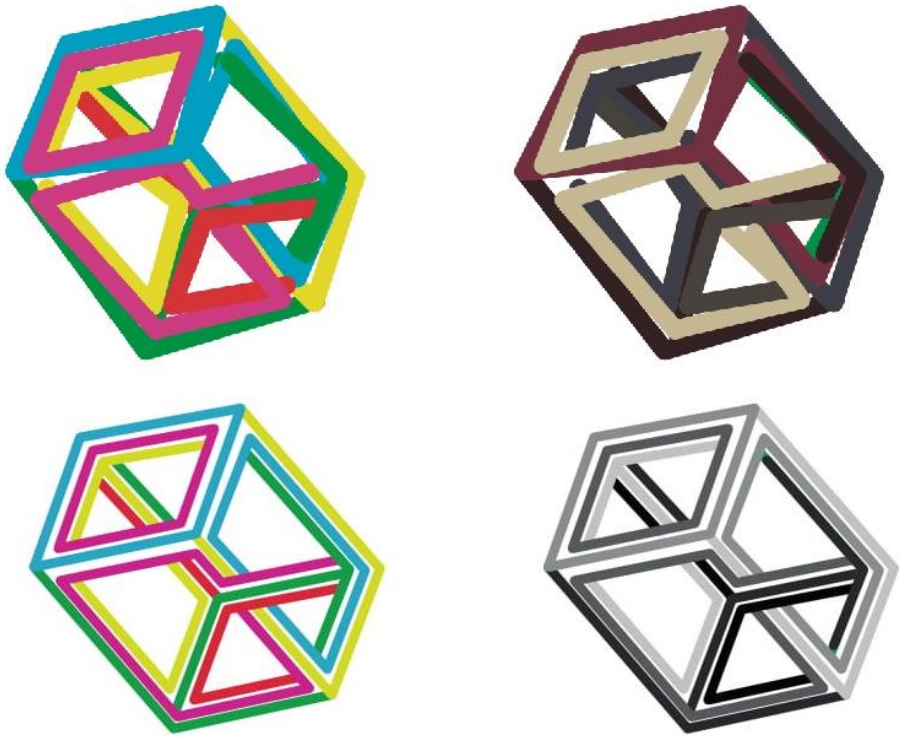
Somos una startup con base en Buenos Aires, Argentina y Polonia, y diseñamos e implementamos soluciones de :

- Big Data + Machine Learning
- Cloud
- UX/UI y Aplicaciones Móviles para Big Data apps.
- Consultoria en Hadoop

Agenda

- El desafio : Que temenos que lograr y a que nos enfrentamos
- Como implementarlo en entornos Big Data
- Arquitecturas Seguras End-to-End
- ¿ Qué puede salir mal ?
- Referencias
- Conclusión

El desafio



El Desafio: Seguridad de los datos

El conjunto de medidas preventivas, de detección y correctivas para proteger la integridad, confidencialidad y disponibilidad de los datos.

CAIN - D

- **C**ONFIDENCIALIDAD
- **A**UTENTICIDAD
- **I**NTEGRIDAD
- **D**ISPONIBILIDAD

} **N**O REPUDIO

- ❑ *AUDITORIA*
- ❑ *TRAZABILIDAD*

Cain and Abel

CAIN - D

- **C**ONFIDENCIALIDAD : La información no puede ser accedida o hecha pública por usuarios no autorizados.
- **A**UTENTICIDAD : El origen de la información es verificable.
- **I**NTEGRIDAD : La información es correcta y completa donde todo su ciclo de vida.
- **N**O REPUDIO : Las partes de una transacción de datos no pueden negar su participación en la misma.
- **D**ISPONIBILIDAD : La información está disponible cuando se la requiera.

El Desafio : Amenazas a la información sensible

Amenazas Tecnologícas Emergentes

- Botnets
- Dispositivos IoT inseguros
- DDoS (Distributed Denial of Service Attack)

Ej : XBASH attack

Amenazas Internas

- Acciones no intencionales
- Usuarios Maliciosos

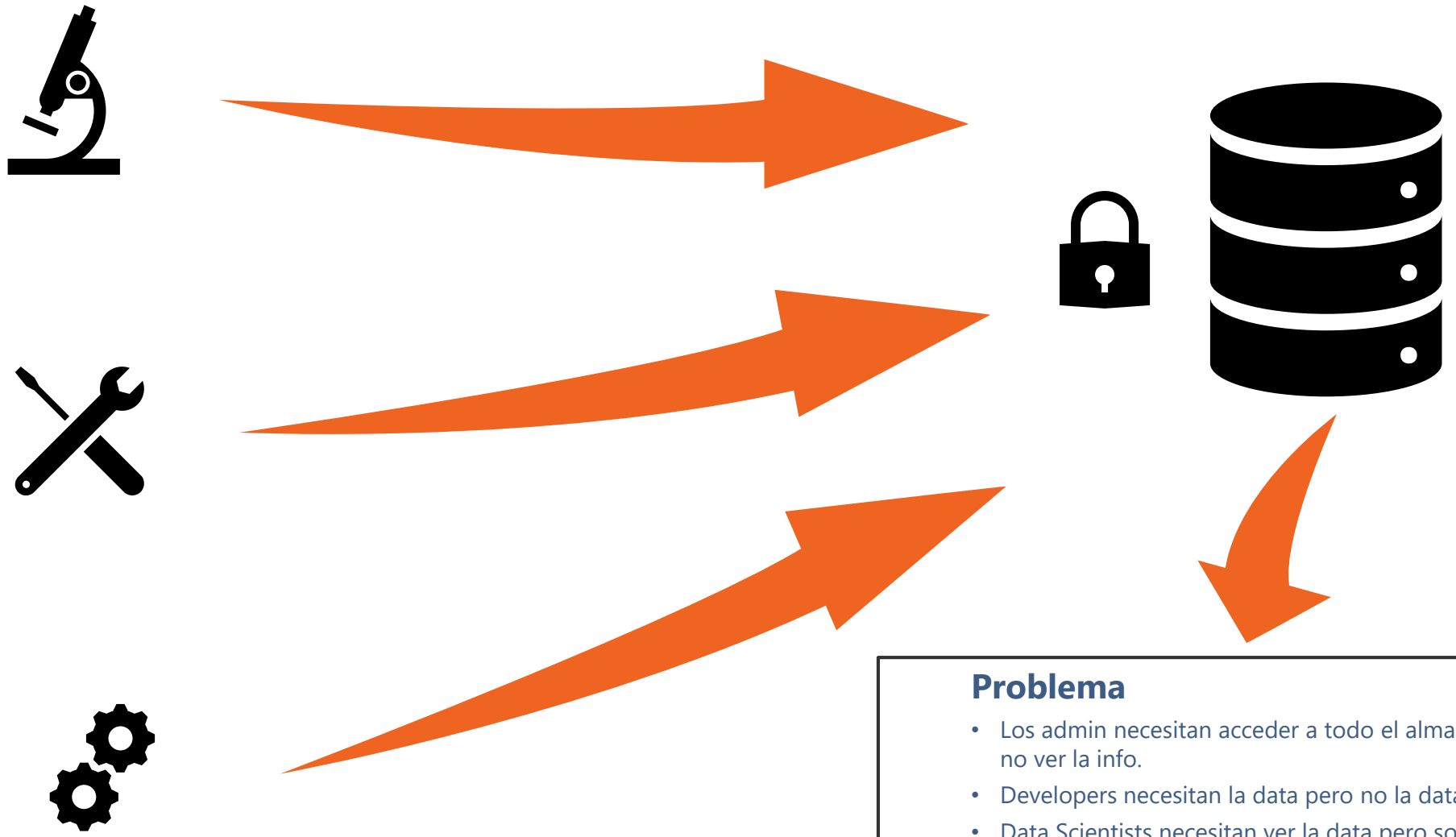
Desafios Regulatorios

- Regulaciones que varian periodicamente
- EUROPA : GDPR

Objetivo

- Datos Sensibles
- Credenciales de Acceso
- Recursos de las plataformas Big Data

El Desafio : Distintos tipos de usuarios, misma plataforma



Problema

- Los admin necesitan acceder a todo el almacenamiento pero no ver la info.
- Developers necesitan la data pero no la data sensible
- Data Scientists necesitan ver la data pero solo en forma especifica

Mejores Prácticas

Organización

- DSO
- Guias de usuario
- Políticas de acceso
- Gobierno
- …

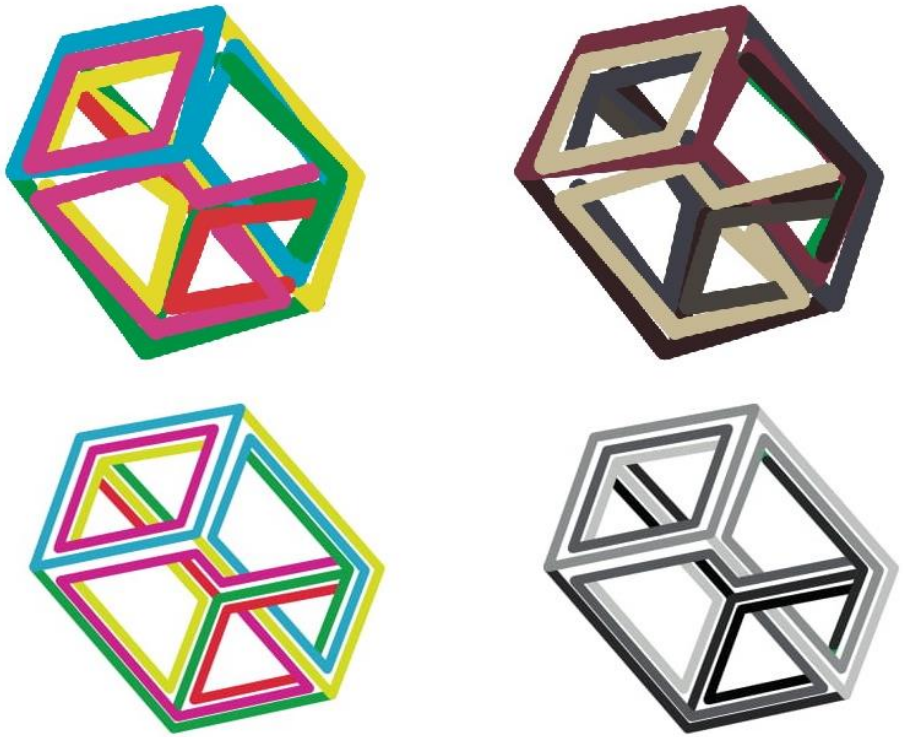
Humana

- Concientización
- Capacitación
- …

Tecnológica

- Redes
- Actualización de software
- Protección de datos
- Auditoría
- …

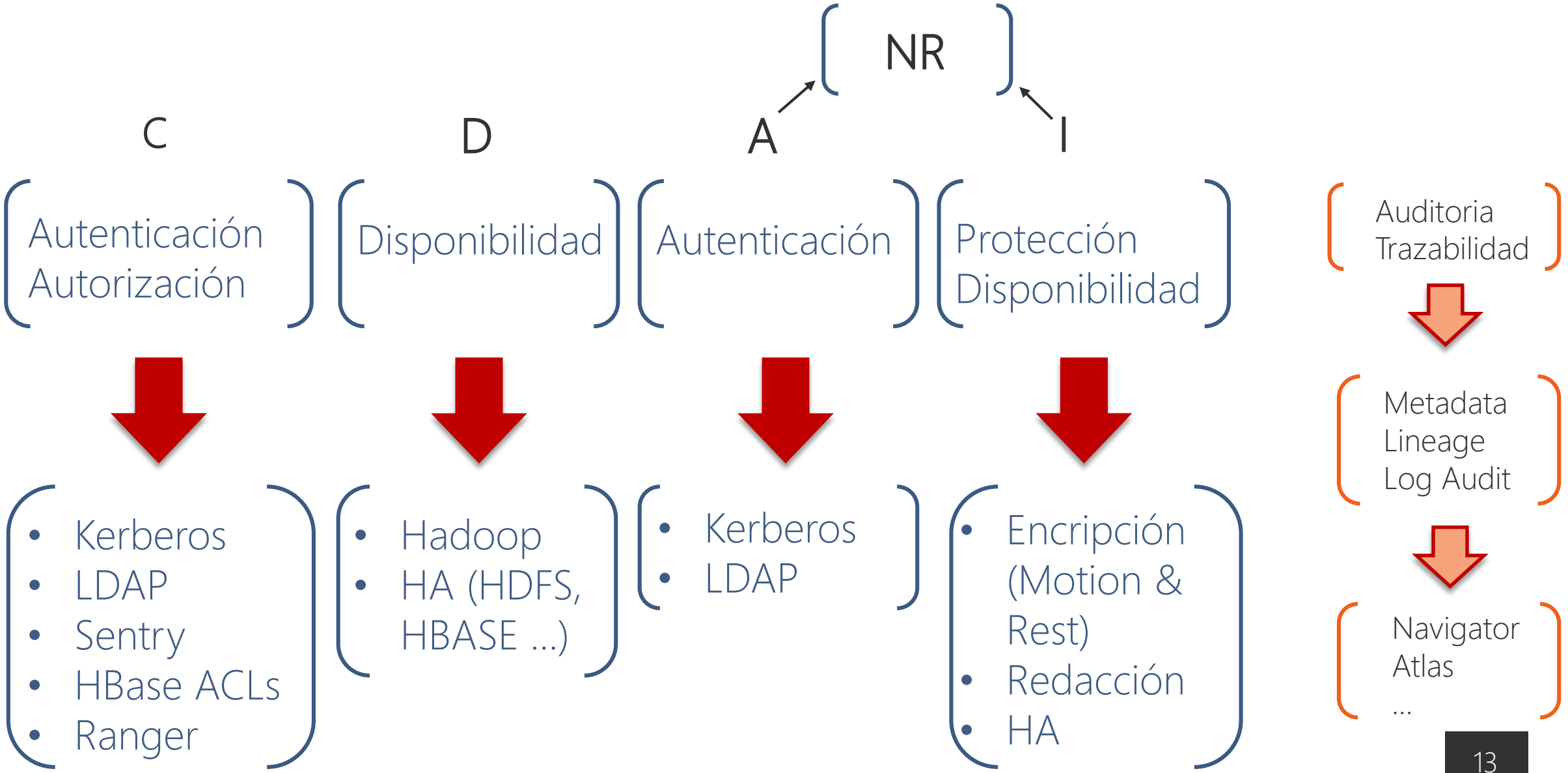
Como implementarlo en Big Data



De los conceptos a la tecnología

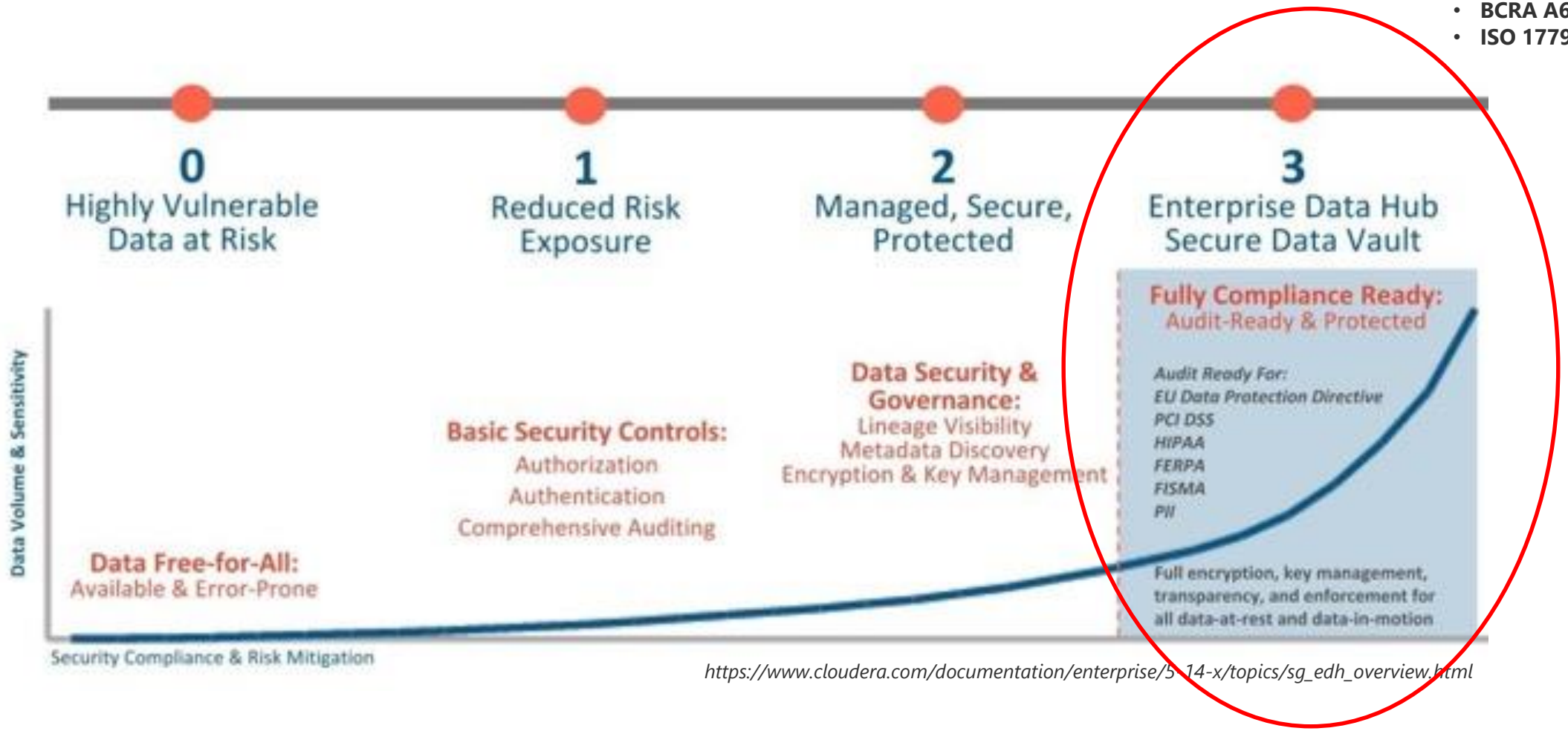
- AUTENTICACION : Identifica la identidad del usuario.
- AUTORIZACION : Habilita el acceso a los usuarios.
- PROTECCION : Protege los datos de ser usados excepto por usuarios autorizados.
- DISPONIBILIDAD : Hace los datos accesibles cuando se necesitan.

De los conceptos a la tecnologias



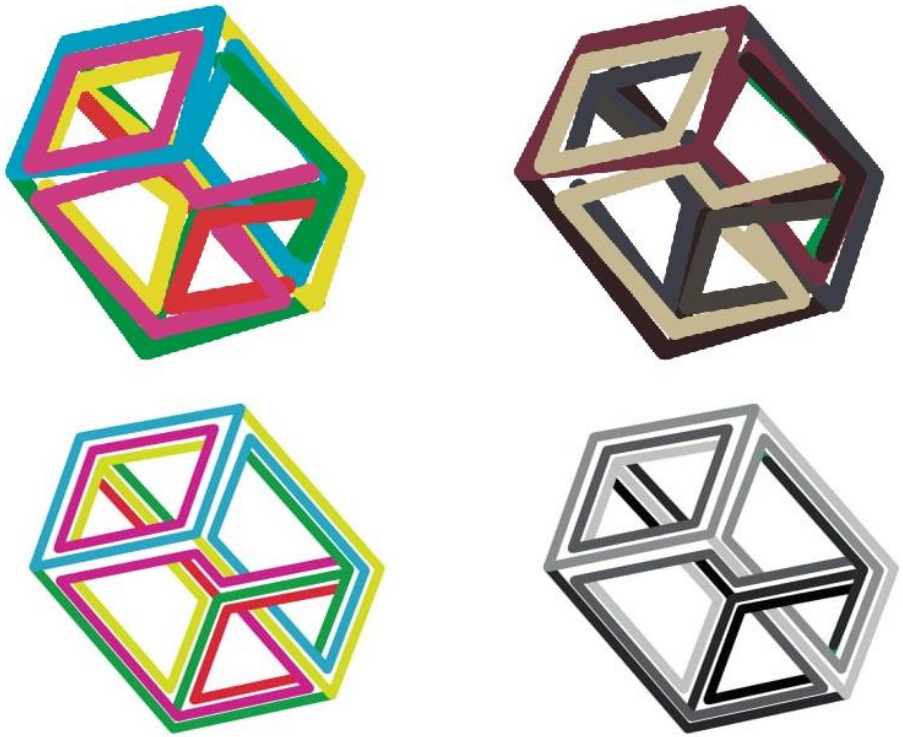
De los conceptos a la tecnologias

- **BCRA A6375**
- **BCRA A6495**
- **ISO 17799/27001**

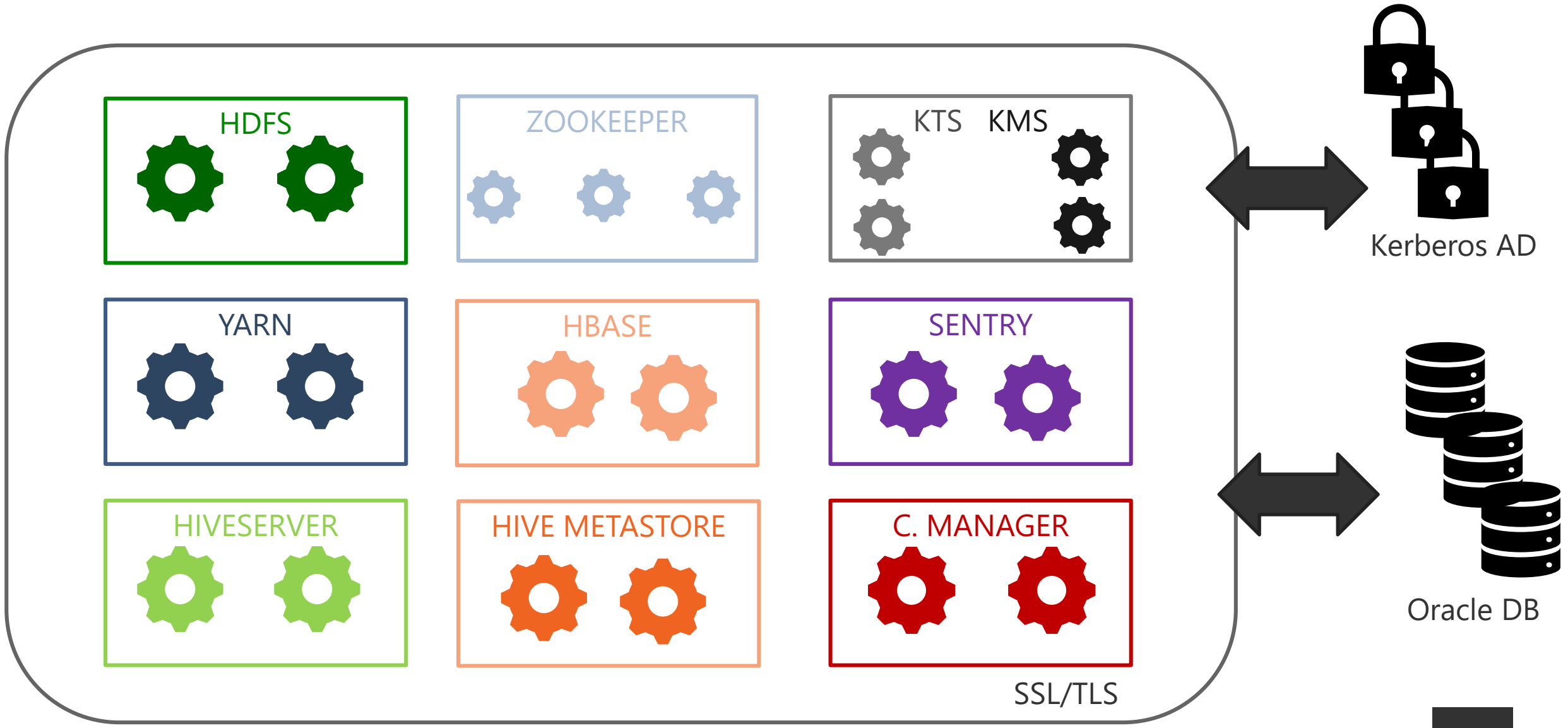


https://www.cloudera.com/documentation/enterprise/5-14-x/topics/sg_edh_overview.html

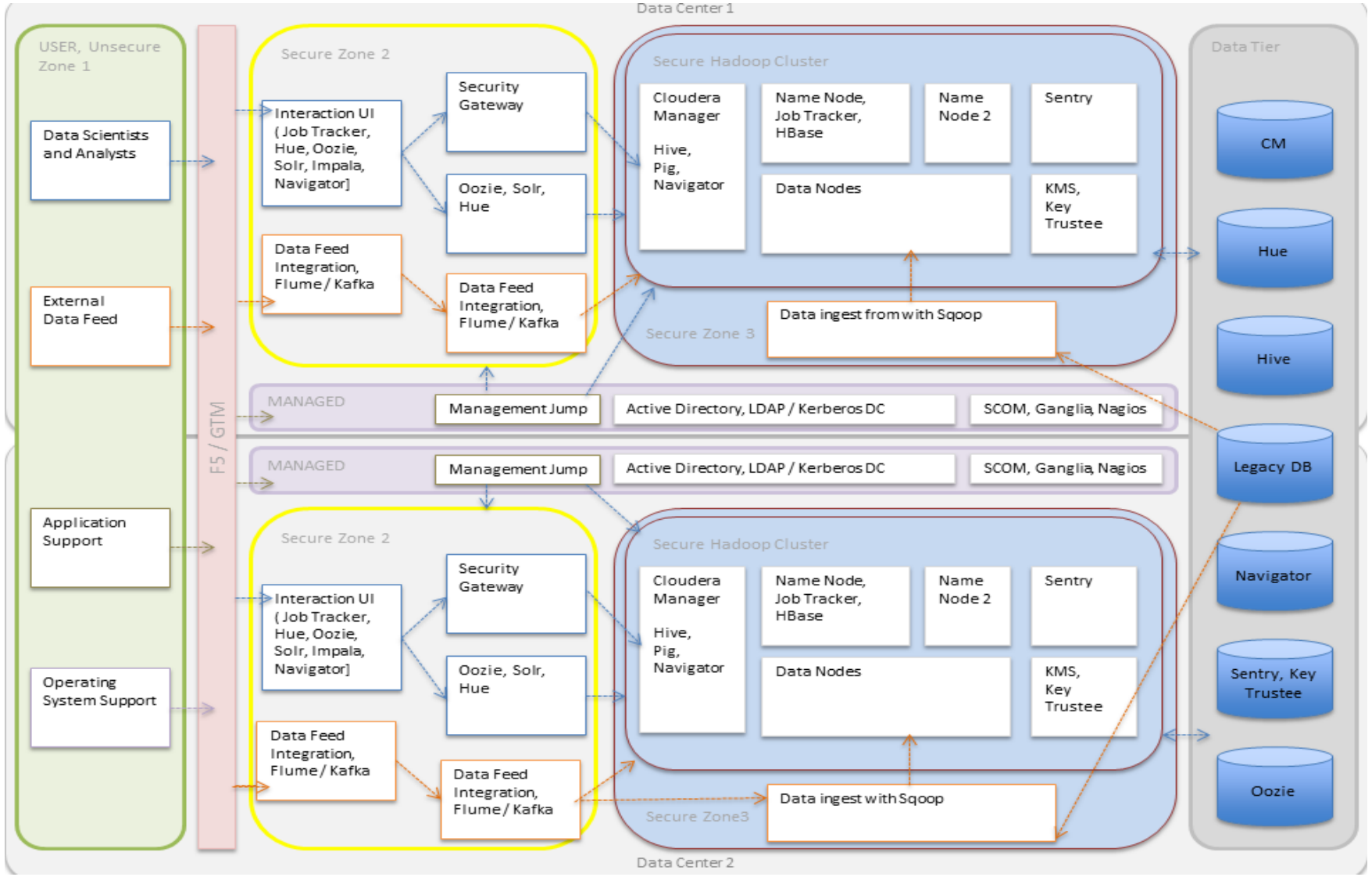
End-to-End Arquitecturas Seguras



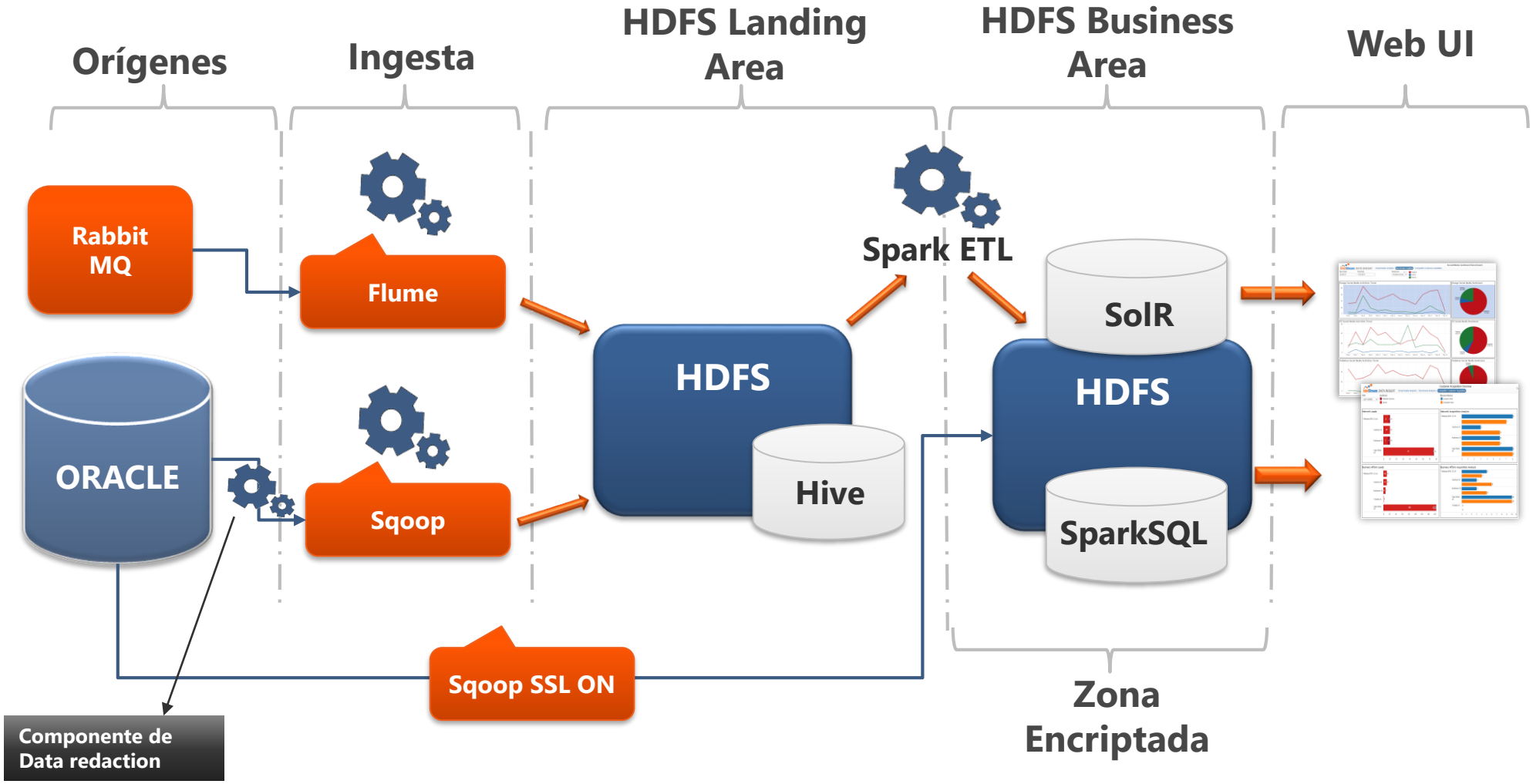
Ej : Infraestructura Segura en Cloudera



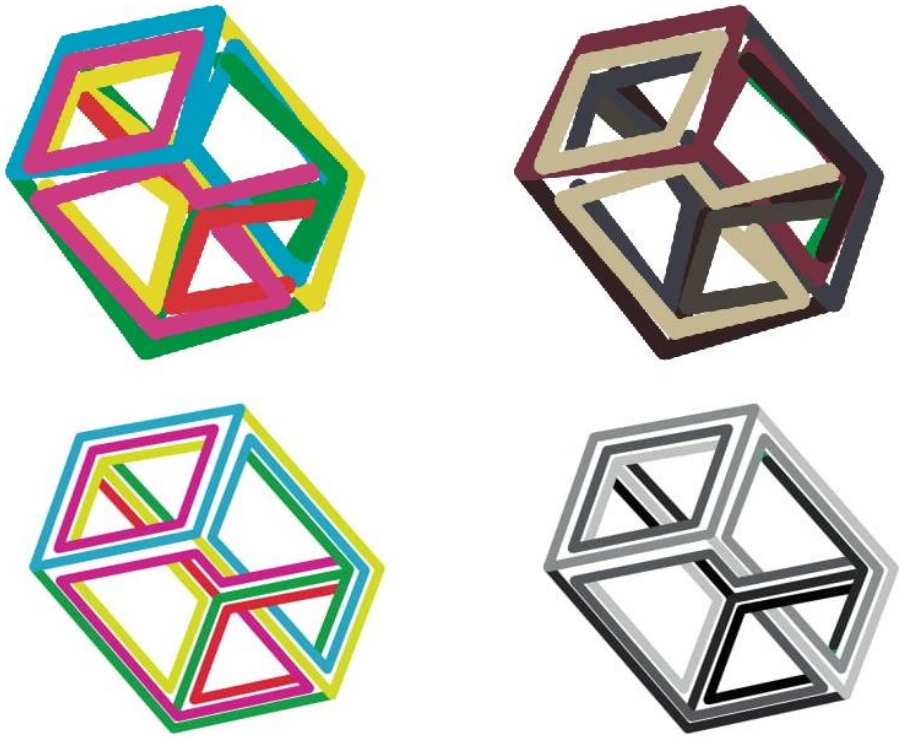
La infraestructura completa



Arquitectura Segura en Big Data



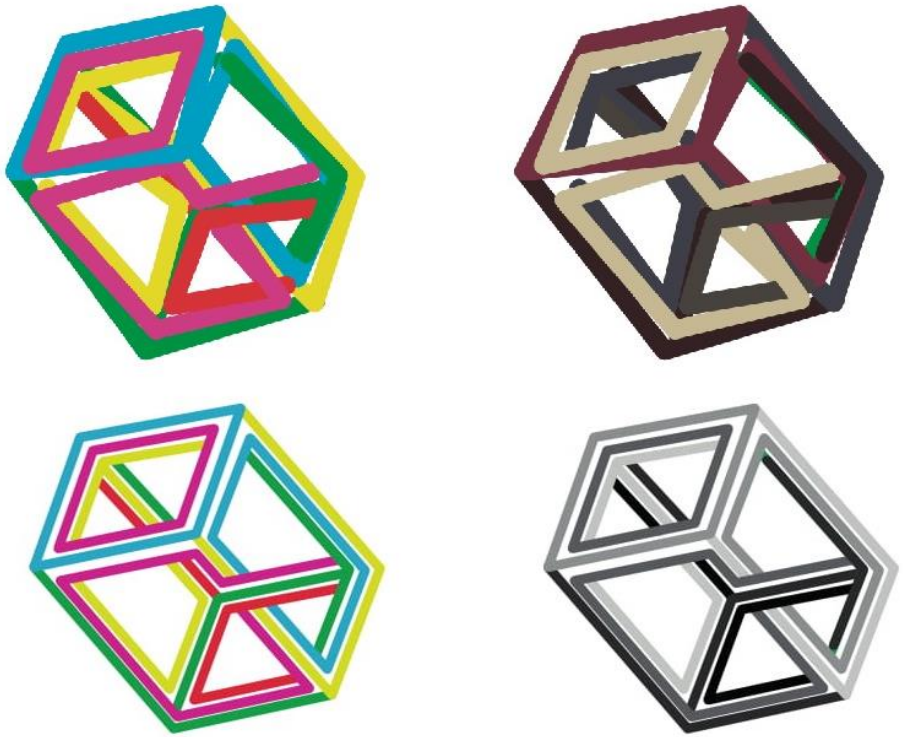
Cosas que pueden salir mal



¿ Que puede salir mal ? Siempre hay malas noticias

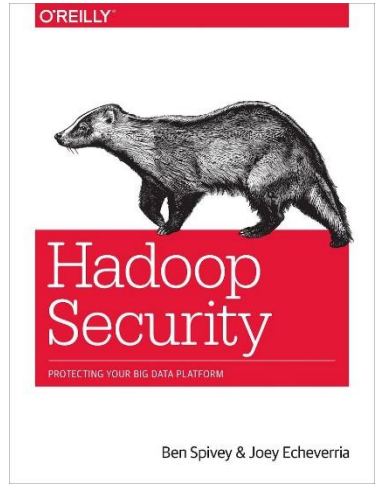
- LAS APLICACIONES INSEGURAS NO FUNCIONAN EN ENTORNOS SEGUROS 
- Para usar el wizard de Kerberos, se necesita un usuario de privilegios altos 
- SparkSQL no respeta la autorización configurada 
- Habilitar autorización en Hive deshabilita la característica de “Impersonation” 
- Spark Streaming no podia consumir de un Kafka con SSL+Kerberos 

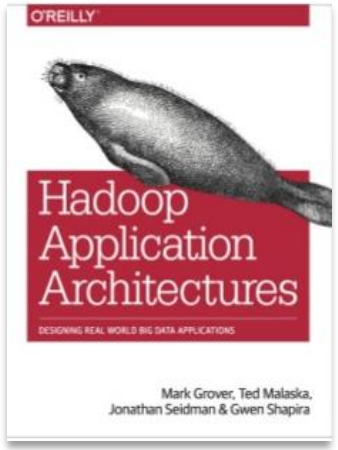
Referencias

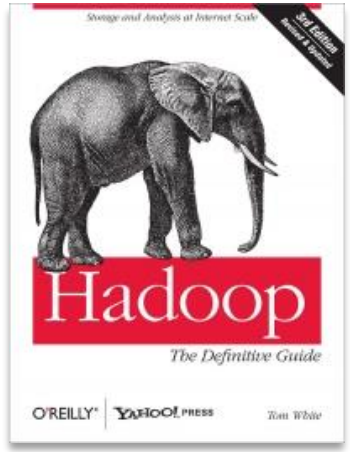


References

- ✓ https://en.wikipedia.org/wiki/ISO/IEC_27002
- ✓ http://web.iram.org.ar/index.php?vernorma&id=2439
- ✓ https://www.cloudera.com/documentation/enterprise/latest/PDF/cloudera-security.pdf
- ✓ https://www.cloudera.com/documentation/enterprise/5-9-x/topics/security.html
- ✓ https://www.forbes.com/sites/gregorymcneal/2014/05/26/banks-challenged-by-cybersecurity-threats-state-regulators-acting/#228d745597f7







BIG DATA WEEK
A GLOBAL FESTIVAL OF DATA

ReactoData

¡ Gracias !

Preguntas, sugerencias y comentarios en “Ask the expert”