SEMINARIO

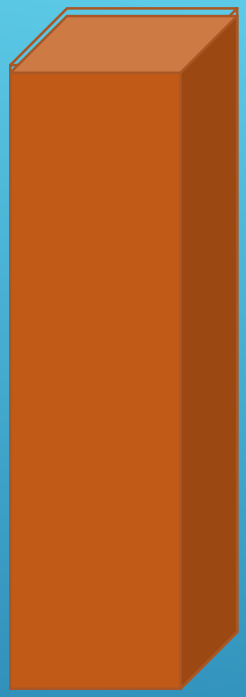
e-AIP

PROYECTO RLA/06/901

Oficina Regional Sudamericana
(SAM) - OACI

Juan José González Pose
Lic. Análisis de Sistemas de Información

Lima, 01 al 04 de Noviembre, 2016



GESTIÓN DE LA BASE DE DATOS

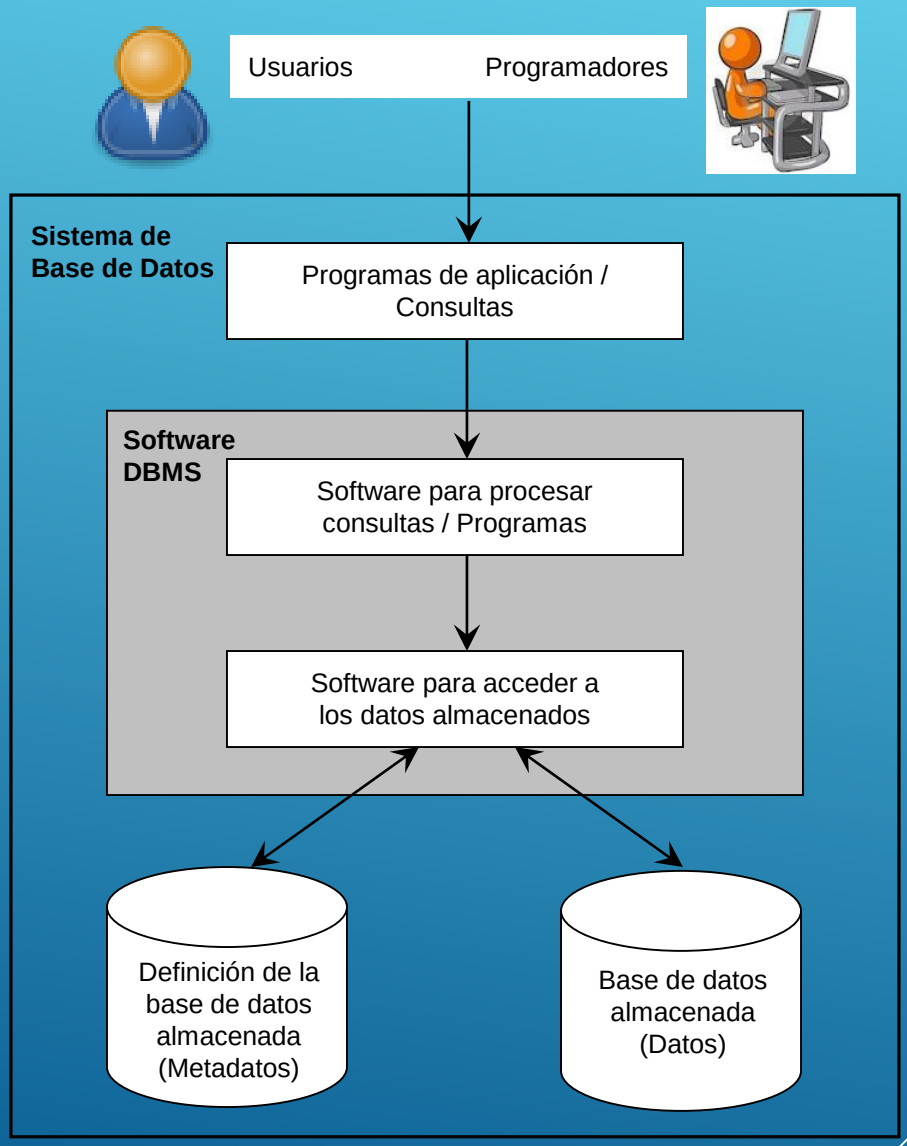
MENÚ

- CREDENCIALES PARA EL ACCESO A LA e-AIP
- ACCESO PARA USUARIOS REGISTRADOS
- NIVELES DE ACCESOS PARA USUARIOS NO REGISTRADOS.
- PROTECCIÓN DEL DATO.
- PROTECCIÓN DE LOS DERECHOS DEL ORIGINADOR DEL DATO.

SISTEMA DE GESTIÓN DE BASE DE DATOS

- Colección de programas (software) que permite a los usuarios crear y mantener una Base de Datos.
- Se los conoce también como SGBD o DBMS.
- Estos programas facilitan los procesos de:
  - Definición: tipos de datos, estructuras, restricciones (metadatos en general)
  - Construcción: almacenamiento controlado de los datos
  - Manipulación: consultas y actualizaciones de datos
  - Compartición: acceso controlado y simultáneo a los datos por parte de varios usuarios
  - Protección: contra el mal funcionamiento de los programas o equipos (software o hardware) y control de acceso a los datos por parte de personal no autorizado

ENTORNO DE UN SISTEMA DE BASE DE DATOS SIMPLIFICADO



COMPONENTES DE UN SGBD

- **Lenguaje de definición de datos** (DDL – Data Definition Language)
  - Es utilizado para describir todas las estructuras de la información y los programas que se usan para construir, actualizar e introducir la información que contiene una base de datos.

- **Lenguaje de manipulación de datos** (DML – Data Manipulation Language)
  - Es utilizado para escribir programas que crean, actualizan y extraen información de la base de datos.

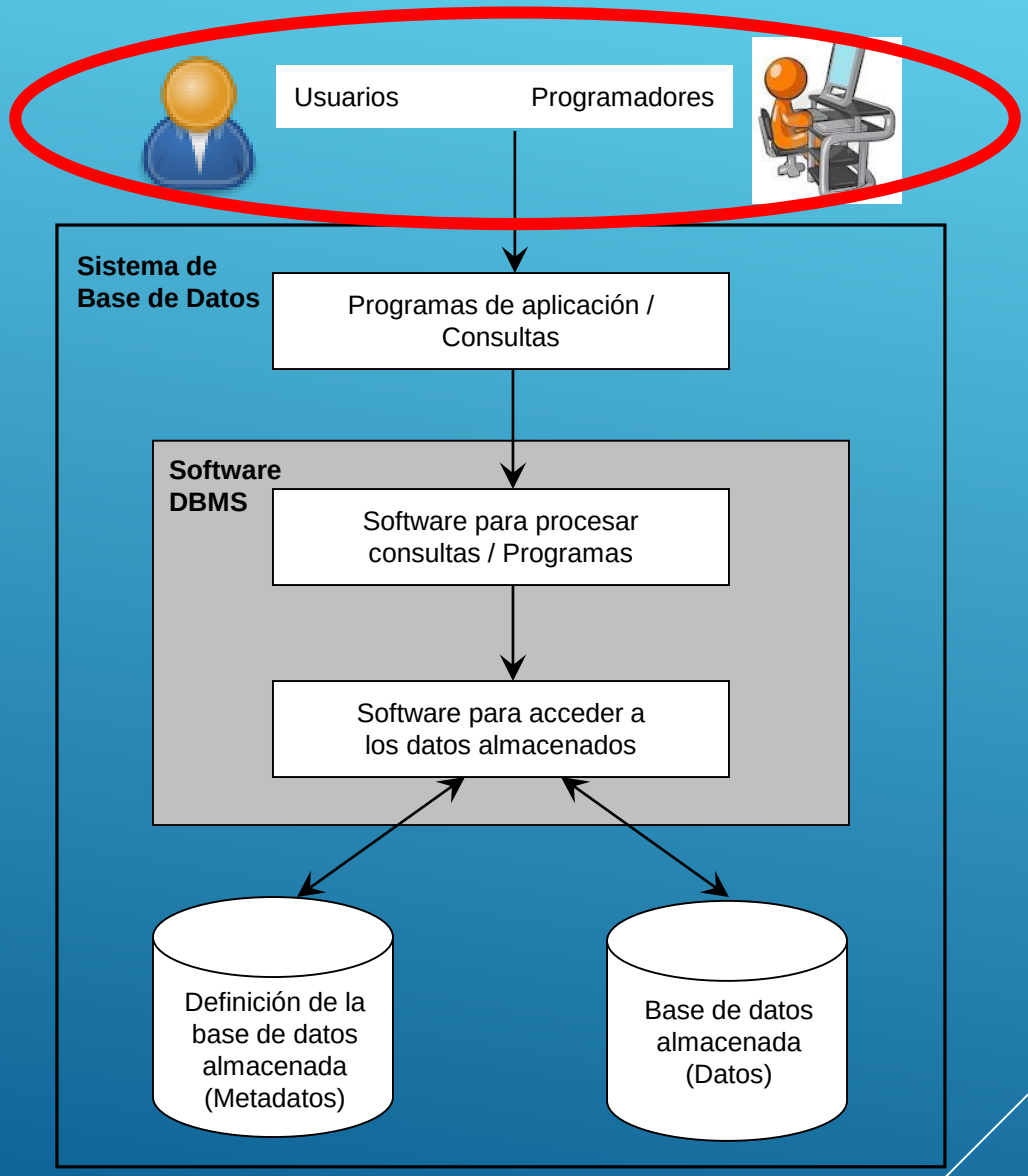
OBJETIVOS DE UN SGBD

- Control de la redundancia de datos.
- Evitar inconsistencia de los datos.
- Accesibilidad a los datos.
- Seguridad de los datos.
- Integridad de los datos.
- Evitar anomalías en el acceso concurrente.
- Recuperación de fallos.
- Información distribuida.

ALGUNOS DBMS

- Comerciales:
  - SQL Server
  - Oracle
  - Sybase ASE
  - Informix
  - DB2 ...
- Libres:
  - MySQL
  - PostgreSQL
  - Sybase (para Linux) ....

TIPO DE USUARIOS DE UN SISTEMA DE BASE DE DATOS



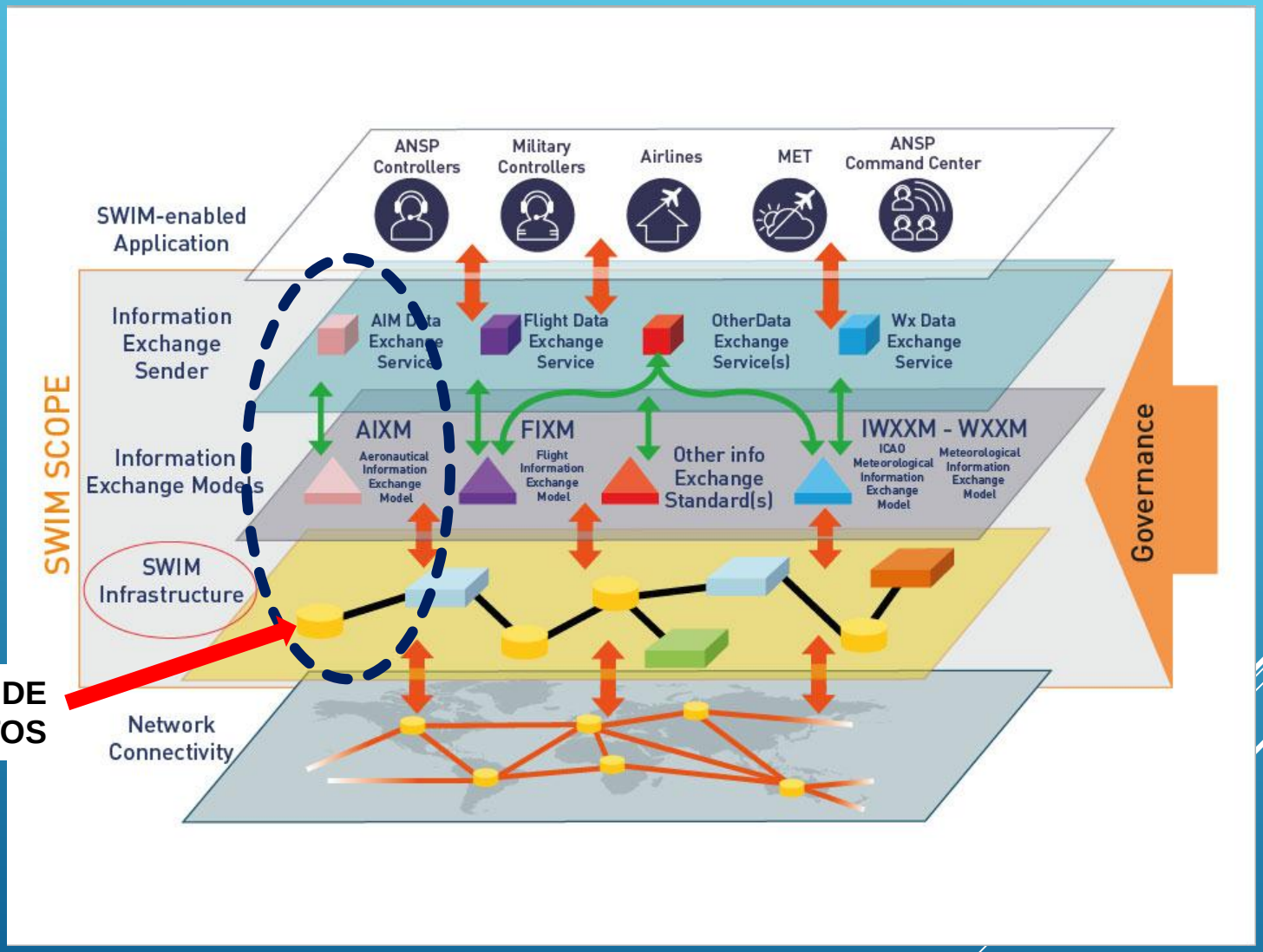
TIPO DE USUARIOS DE UN SISTEMA DE BASE DE DATOS

- **Usuarios finales**: son usuarios que interactúan con el sistema mediante un programa de aplicación con una interfaz de formularios.
- **Programador de aplicaciones**: son profesionales informáticos que escriben los programas de aplicación, utilizando herramientas para desarrollar interfaces de usuario.
- **Usuarios expertos**: son usuarios sofisticados que escriben aplicaciones de bases de datos especializadas y adecuadas para el procesamiento de datos tradicional.
- **Administrador de Base de Datos**: Tienen el control central del SGBD.

FUNCIONES DEL ADMINISTRADOR DE LA BASE DE DATOS

- Definición del esquema de la base de datos
- Definición de la estructura y el método de acceso
- Modificación del esquema y la organización física
- Concesión de autorización para el acceso a los datos
- Mantenimiento rutinario.

BASE DE DATOS EN EL ENTORNO SWIM



EXPECTATIVAS

- Los datos son correctos
  - El usuario siempre espera ver los datos correctos
- Los datos tienen que estar disponibles cuando los necesito
  - Todos pueden querer acceder al mismo tiempo
  - No importa que falle el hardware, que haya un apagón o incendio
- Los datos son para mí y mis socios
  - Sólo los usuarios debidamente autorizados pueden consultar y modificar los datos
- Los tiempos de respuesta deben ser aceptables
- Los datos almacenados en una Base de Datos son importantes y tienen un sentido específico para un conjunto determinado de usuarios

SEGURIDAD DE ACCESO A LA BASE DE DATOS

- El objetivo del sistema de seguridad es preservar o maximizar las siguientes propiedades:
  - **Confidencialidad** (**C**onfidenciality): conjunto de reglas que limitan el acceso a la información. Ningún sujeto debe realizar operaciones de lectura sobre objetos que no tenga autorizados.
  - **Integridad** (**I**ntegrity): garantía que la información es confiable y precisa. La información no debe corromperse de ninguna forma, ya sea intencional o accidentalmente.
  - **Disponibilidad** (**A**vailability): garantía de un acceso fiable a la información por personas autorizadas. La información debe estar accesible cuando sea requerida por parte de sujetos autorizados.

SEGURIDAD DE ACCESO A LA BASE DE DATOS

- Una amenaza es la posibilidad de perder alguna de las propiedades:
  - **Confidencialidad** : Es la posibilidad de acceso no autorizado.
    - Ejemplo: si un usuario logra consultar una relación a la que no se le otorgó privilegios .
  - **Integridad** : Es la posibilidad del cambio de datos no autorizado.
    - Ejemplo: cambiar de forma no autorizada el resultado de un examen.
  - **Disponibilidad** : Es la posibilidad de que la información no esté disponible cuando sea requerida.
    - Ejemplo: si un usuario mal intencionado logra privilegios altos y quita privilegios de acceso a los usuarios.

NIVELES DE SEGURIDAD

- **Nivel Físico**:
  - El lugar físico donde se encuentra la BD debe estar protegido contra personas no autorizadas.
- **Nivel de Software**:
  - La BD debe estar protegida con un Sistema Operativo que valide usuarios, etc.
- **Nivel de Base de Datos**:
  - Asignación de permisos, vistas, etc.

NIVELES DE SEGURIDAD - FÍSICO

- **Nivel Físico**:
  - El lugar físico donde se encuentra la BD debe estar protegido contra personas no autorizadas.
    - ¿Qué ocurriría si alguien accede a los datos y los modifica de ex profeso?
    - ¿Cuáles serían las consecuencias?
    - ¿Cómo debería ser el acceso?
    - ¿Control físico (guardias), cámaras de control y registro, cerraduras electrónicas, elementos biométricos?
  - Analizar qué es lo que se necesita según el caso.

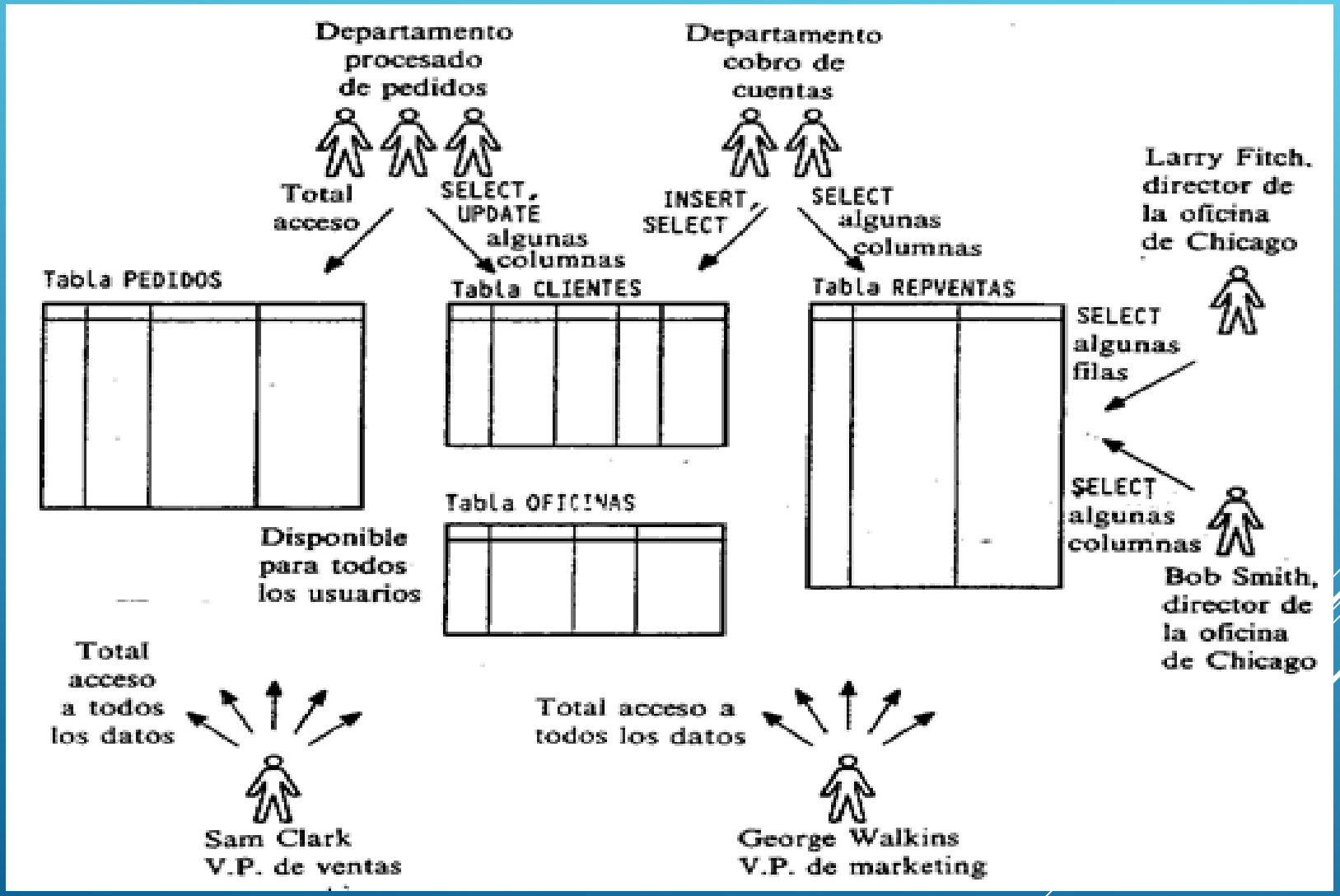
NIVELES DE SEGURIDAD - SOFTWARE

- **Nivel de Software**:
  - La BD debe estar protegida con un Sistema Operativo que valide usuarios, etc.
    - ¿Qué política de contraseña maneja su sistema?
    - ¿Qué clase de usuarios maneja su sistema?
    - ¿Cómo quedan las sesiones de trabajo de cada usuario al finalizar su jornada?
    - ¿Ocurre que un usuario se encuentra trabajando bajo la sesión de otro usuario?
  - Analizar qué es lo que se necesita según el caso.

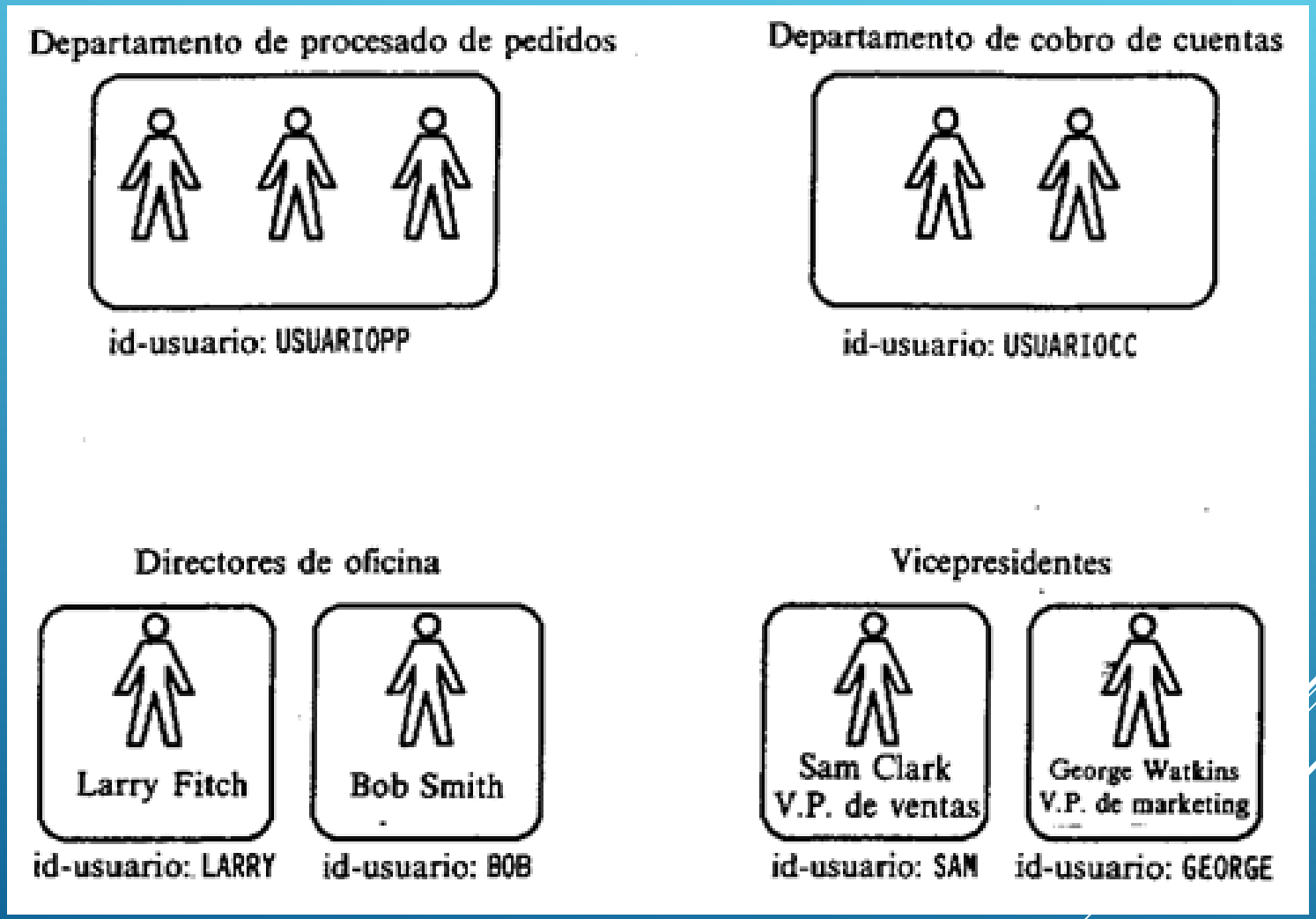
NIVELES DE SEGURIDAD – BASE DE DATOS

- En un esquema de seguridad para Base de Datos intervienen, al menos, 3 conjuntos de elementos básicos:
- **Sujetos o actores**
  - Actores (personas, software, etc.) que pueden realizar operaciones sobre los objetos.
- **Objetos**
  - Los datos, la información, la base de datos (su esquema e instancia). Los Objetos que son manejados por los Sujetos a través de las operaciones.
- **Operacione**s
  - Lectura (consulta), escritura, modificación, asignación de permisos. Las operaciones que pueden realizar los Actores sobre los Objetos. Deben considerarse también las reglas que sean necesarias para garantizar la seguridad con respecto a los Objetos

INTERACCIÓN ENTRE PARTICIPANTES



USUARIOS


Departamento de procesado de pedidos
id-usuario: USUARIOPP
Departamento de cobro de cuentas
id-usuario: USUARIOCC
Directores de oficina
Larry Fitch
id-usuario: LARRY
Bob Smith
id-usuario: BOB
Vicepresidentes
Sam Clark
V.P. de ventas
id-usuario: SAM
George Watkins
V.P. de marketing
id-usuario: GEORGE

ESQUEMAS DE SEGURIDAD

- Hay tres esquemas que se manejan en bases de datos:
  - **Control de Acceso Discrecional** (Discretionary Access Control – DAC)
  - **Control de Acceso Basado en Roles** (Role Based Access Control – RBAC)
  - **Control de Acceso Obligatorio** (Mandatory Access Control – MAC)

CONTROL DE ACCESO DISCRECIONAL (DAC)

- En el esquema DAC, el DBA simplemente asigna o quita privilegios a los usuarios de la base de datos sobre ciertos objetos.
- Existen:
  - Sujetos: usuarios o grupos de usuarios.
  - Objetos: recursos del sistema, a saber, Database, Schema, Tablas, Vistas, Procedimientos
  - Permisos o Privilegios: autorización dada a un sujeto para realizar una determinada operación sobre un objeto dado.
- Cada “objeto” debe tener un “dueño” y es éste el que asigna el permiso para su uso

CONTROL DE ACCESO DISCRECIONAL (DAC)

- La seguridad en la BD la define el DBA o un encargado de seguridad de acuerdo a las posibilidades del DBMS y las necesidades de la organización.
- Para eso realiza entre otras, las siguientes tareas:
  - Creación de usuarios: es la forma de definir a los sujetos.
    - Ejemplo: crear el usuario “Pepe”
  - Asignación / Eliminación de Privilegios.
    - Ejemplo: “Pepe” puede leer la información de la Tabla Salarios
- Significa, entonces, que el usuario “Pepe” puede acceder al objeto “Tabla Salarios” de acuerdo con los privilegios (lectura) otorgado.

CONTROL DE ACCESO DISCRECIONAL (DAC)

- Hay dos niveles de privilegios:
  - Nivel de Base de Datos (o de cuenta):
    - Son especificaciones generales de qué puede o no hacer determinado sujeto.
    - Ej.: Si un usuario tiene el privilegio CREATE TABLE entonces puede crear tablas.
  - Nivel de Relación (o tabla):
    - Es un nivel de granularidad más fino: tabla, vista o incluso atributos.
    - Ej.: Si un usuario tiene el privilegio SELECT sobre una tabla “A”, entonces puede consultar dicha tabla.

CONTROL DE ACCESO DISCRECIONAL (DAC)

- Un mecanismo que implemente DAC debe ser capaz de responder la siguiente pregunta:
  - ¿Tiene el sujeto "S" privilegios "r" para acceder al objeto "O"?
- Si la respuesta es "si", entonces "S" puede acceder a "O". En caso contrario, no podrá acceder.
- En general, se plantea una matriz de sujetos y objetos donde en la intersección se indica el privilegio.
- Privilegios: r = lectura, w = escritura, x = ejecución

	Objeto		
Sujeto	Tabla Sueldo	Tabla Datos Personales	Vista Teléfonos
Luis	-	x	r
Alejandra	r	-	rwx
Karina	rwx	rwx	rwx

CONTROL DE ACCESO BASADO EN ROLES (RBAC)

- Se propone como una alternativa más flexible, pero igual de segura que DAC.
- Básicamente consiste en la creación de roles para los trabajos o funciones que se realizan en la organización.
- Los miembros del staff se asignan a roles y a través de estos roles adquieren permisos para ejecutar funciones del sistema.
- La pertenencia de un usuario a un rol, puede llegar a ser dinámica, por lo que se suele manejar el concepto de “sesión”.

CONTROL DE ACCESO BASADO EN ROLES (RBAC)

- Rol: es el conjunto de acciones y responsabilidades asociadas con una actividad en particular.
- Se define una jerarquía de roles.
- Los sujetos pertenecen a uno o más roles.
- Se asignan privilegios sobre los objetos a los roles, y no directamente a los sujetos.
- Se requieren mecanismos para:
  - Identificar los roles en un sistema y asignar los sujetos a los roles definidos.
  - Establecer los permisos de acceso a los objetos para cada rol.
  - Establecer permisos a los sujetos para que puedan adoptar roles.

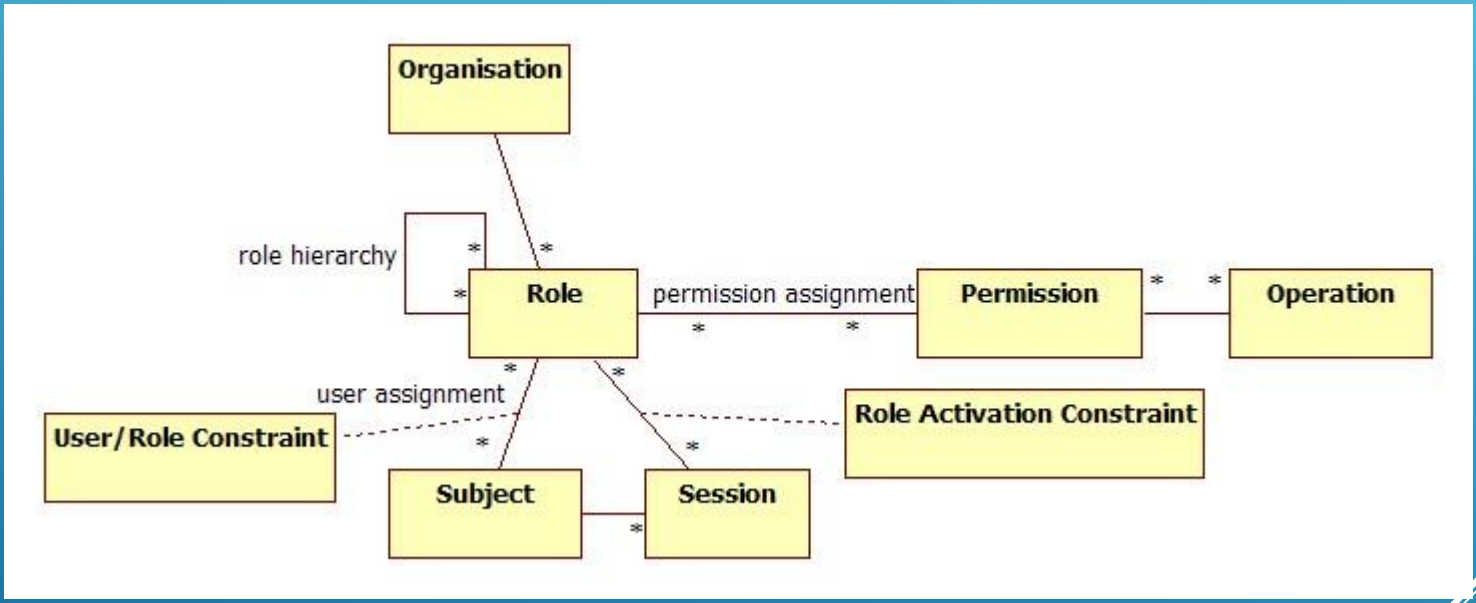
CONTROL DE ACCESO BASADO EN ROLES (RBAC)

	Objeto		
Rol	Tabla Sueldo	Tabla Datos Personales	Vista Teléfonos
Read-Only	-	x	r
Product-Creator	r	-	rwx
Full Access	rwx	rwx	rwx

	Rol		
Usuario	Read-Only	Product-Creator	Full Access
Luis	Si	No	No
Alejandra	No	Si	No
Karina	No	No	Si

CONTROL DE ACCESO BASADO EN ROLES (RBAC)

- Si se consideran los roles, sesiones, sujetos, permisos y operaciones que se pueden realizar, tendríamos:



CONTROL DE ACCESO OBLIGATORIO (MAC)

- Es una política de control de acceso determinada por el sistema no por el dueño de un recurso. Clasifica a sujetos y objetos en niveles de seguridad.
- Se utiliza en sistemas multinivel que procesan información altamente sensible.
- Sistema multinivel: es un sistema de computadoras que maneja múltiples niveles de clasificación entre sujetos y objetos, como por ejemplo información gubernamental o militar.

CONTROL DE ACCESO OBLIGATORIO (MAC)

- Se define un conjunto ordenado de niveles de seguridad. Ejemplo: Modelo Bell-LaPadula:
  - Top Secret(TS) > Secret(S) > Confidential(C) > Unclasified(U)

- A cada sujeto “S” se le asigna uno de estos niveles o clases (class(S))
- A cada objeto “O” se le asigna uno de estos niveles o clases (class(S)).

REGLAS BELL - LA PADULLA

- Propiedad de Seguridad Simple:
  - Un sujeto “S”, sólo puede leer aquellos objetos “O” tales que class(S) ≥ class(O)
  - Un sujeto puede leer objetos de su nivel de seguridad o inferior, pero nunca de niveles superiores.
  - Garantiza que un sujeto no puede leer información a la que no tiene derecho (más confidencial).
- Propiedad Estrella (* property):
  - Un sujeto “S”, sólo puede escribir aquellos objetos “O” tales que class(S) ≤ class(O)
  - Un sujeto puede escribir objetos de su nivel de seguridad y superiores, pero nunca de los niveles inferiores.
  - Garantiza que un sujeto no puede filtrar información a quien no tiene derecho.

SEGURIDAD DE LA INFORMACIÓN

- La Seguridad de la Información es un proceso en el que debemos combinar distintas medidas de seguridad para conseguir nuestro objetivo.
  - Disponer de una política de Seguridad de la Información.
  - Contar con un sistema de identificación para la información específica que debe protegerse.
  - Mantener procedimientos para la protección y el control de la información protegida.
  - Un sistema de alerta y aviso que advierta sobre la sensibilidad de la información y los requisitos establecidos para el manejo de la misma.
- Apoyarnos en las normativas y buenas prácticas existentes, como las normas ISO 27001 y 27002 y en las soluciones tecnológicas.

ORIGEN DE LA INFORMACIÓN

- Referenciar los datos/información recibida con su correspondiente originador.
- Mantener actualizados los metadatos.
- Acuerdos de Nivel de Servicio (SLA) con los originadores de datos/información aeronáutica.
- Recepción de la información con CRC (Código de Redundancia Cíclica).
- Enriquecer los modelos de base de datos si es necesario

¿PREGUNTAS HASTA ACÁ?

TESTEO

¿GRADO DE CANSANCIO DE LA AUDIENCIA?

FIN