



# GT-SCHEMA


## Plan Inicial de securización del directorio

Inmaculada Bravo García ([inma@usal.es](mailto:inma@usal.es))  
Universidad de Salamanca

# Agenda

01. Genésis
02. Objetivos
03. Amenazas y ataques a un directorio
04. OCIL Interpreter
05. Conclusiones

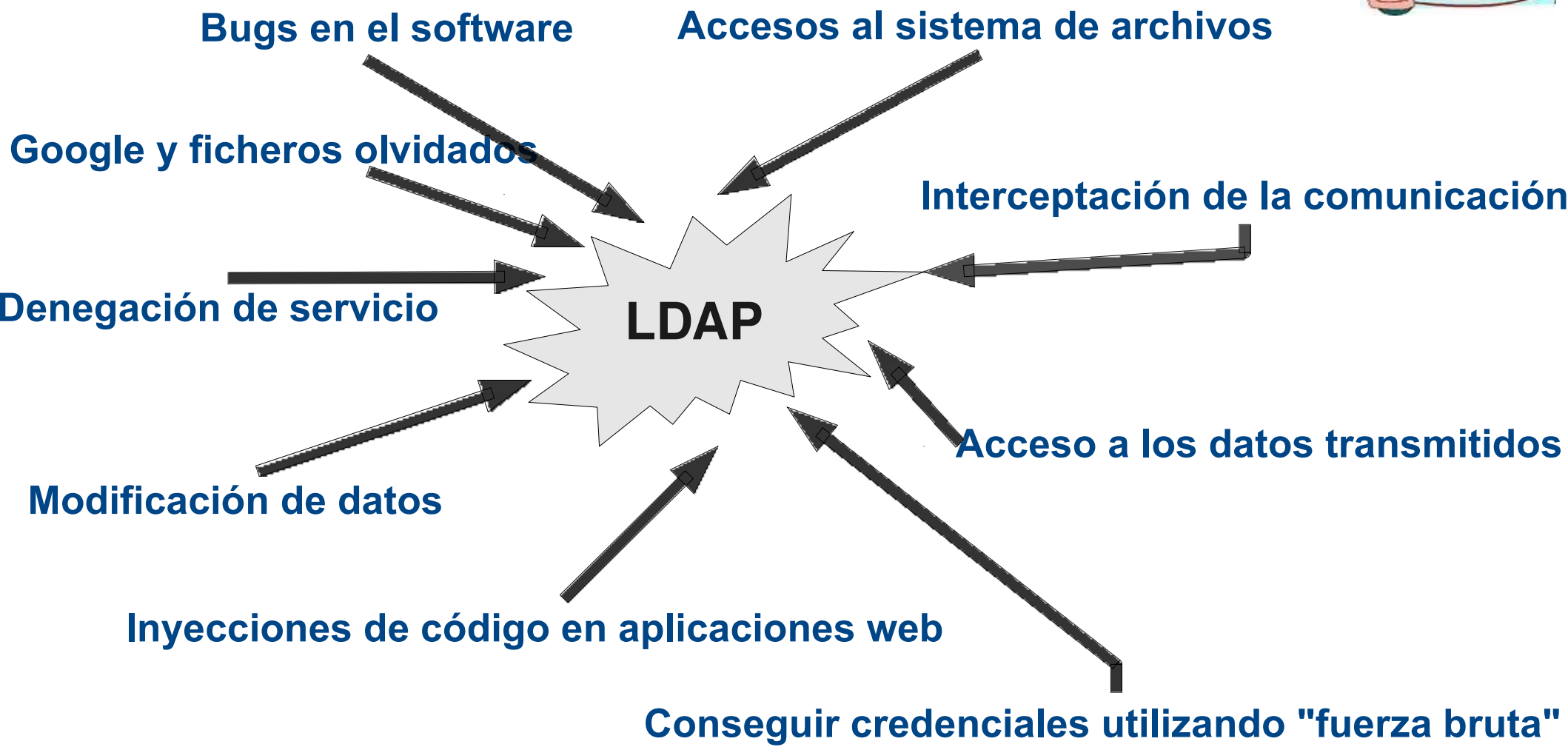
# 01. Génesis del OpenLDAP BSA

- ▶ Estado inicial del directorio
- ▶ Análisis de amenazas
- ▶ Selección de criterios de seguridad
  - Descripción e implantación
  - Valoración
  - Errores frecuentes 
- ▶ Auditoría de su cumplimiento: OCIL Interpreter

## 02. Objetivos del OpenLDAP BSA

- ▶ Mejorar la securización del servicio de directorio.
- ▶ Servir de guía.

## 03. Amenazas y ataques a un directorio



## 03. Amenazas y ataques a un directorio

**Demo**

## 03. Amenazas y ataques a un directorio



¿Y ahora qué podemos hacer?

## 04. SCAP y Lenguaje OCIL

### **SCAP (Security Content Automation Protocol)**

iniciativa del gobierno americano para verificar y automatizar la seguridad.

**OCIL (Open Checklist Interactive Language)** Lenguaje que permite interrogar a un usuario y provee métodos para interpretar las respuestas.

El documento OCIL **OpenLDAP-BSA.xml** es el resultado de codificar los criterios de seguridad propuestos, en XML respetando el Schema OCIL.



# 04. OCIL Interpreter

The screenshot displays the OCIL Interpreter interface. On the left is a tree view of the security plan, with 'ACLs y el rootdn y última condición "by \*none"' selected. The main area shows a 'QUESTION TEST ACTION' window with a 'PASS' status. A table lists the test results:

#	Test Action	Result	Question	Answer
1	ACLs y el rootd...	PASS	¿En las ACLs añ...	false

Below the table, the test details are shown:

Title/Id: ACLs y el rootdn y última condición "by \*none"

Result: PASS

Question: ¿En las ACLs añades al rootdn o la condición "by \*none"?  
Un error común es añadir el rootdn a las ACLs, cuando es un usuario que tiene implícitos permisos totales sobre todo el directorio, las ACLs no afectan al rootdn. Otro error es poner como ultima condición en una ACL " by \*none" la cual también esta implícita y no es necesario escribirla.

Select one:  
 Yes  
 No

Reset

< Previous      Next >

<http://openldap-bsa.forja.rediris.es>



The screenshot shows a Mozilla Firefox browser window displaying the OpenLDAP Baseline Security Analyzer website. The browser title is "OpenLDAP Baseline Security Analyzer - Mozilla Firefox". The website header includes the title "OpenLDAP Baseline Security Analyzer" with a UK flag icon, the subtitle "Plan inicial de securización del directorio", and download links for "OCIL Interprete" and "OpenLDAP-BSA.xml". A large banner features the text "Powered by OpenLDAP" with a mouse cursor pointing to it. On the left, a dark red box contains the text: "Listado de criterios que se deberán tener en cuenta para realizar el plan inicial de securización del directorio." Below this is a list of navigation links: "Introducción", "Ataques a un Directorio", "Criterios de Seguridad", "OCIL Interprete", "Utilización", "Referencias", and "Comentarios". A PDF icon is visible below the links. The main content area has an "Introduction" section with the following text: "EL propósito de este proyecto es elaborar un listado de criterios que se deberían tener en cuenta para realizar el plan inicial de securización del directorio. Se documentan brevemente los principales ataques y las amenazas a las cuales nos enfrentamos los administradores y a continuación se listan los criterios de seguridad que se deben considerar, con una explicación de cada uno, su valoración, como implementarlo y con la etiqueta  se marcan los errores mas comunes que hay que tratar de evitar. Los criterios que se plantean se han recogido de diferentes fuentes que puedes consultar en la sección de [referencias](#) y de la experiencia de administradores LDAP de las instituciones afiliadas a [RedIRIS](#) coordinados a través de la lista IRIS-LDAP. Se utilizará una herramienta gráfica para interrogar al administrador por el

## 05. Conclusiones

- ▶ El directorio es la “*joya de la corona*”
- ▶ Múltiples amenazas
- ▶ Guía de recomendaciones a tener en cuenta
- ▶ Dificultades:
  - Cualquier modificación en el directorio afecta a muchas aplicaciones
  - Reconducir malos hábitos es complicado pero necesario
- ▶ Evolución....

## 05. Evolución

### ▶ GT-SCHEMA

- Adaptarlo a cualquier directorio
- Proponer configuraciones iniciales que recojan todos los ejemplos expuestos
- Evaluar el impacto de las vulnerabilidades a las que nos exponemos por el incumplimiento de estas recomendaciones.

### ▶ Es un proyecto abierto a la colaboración

- Enviando el resultado del cuestionario
- Preguntas
- Comentarios, críticas y correcciones
- etc.



**¿ Alguna pregunta ?**

**Muchas gracias por vuestra atención.**

Inmaculada Bravo (inma@usal.es)