Privacidad en el servicio de directorio

Universidad de Málaga RedIRIS/red.es

Madrid, 12 de diciembre de 2006

Índice

Índice

Índice

Definiciones
¿Contradicciones?. . .

Según el D.R.A.E.

Definiciones

¿Contradicciones?. . .

Según el D.R.A.E.

Directorio

5. m. Guía en la que figuran las personas de un conjunto, con indicación de diversos datos de ellas, como su cargo, sus señas, su teléfono, etc.

Definiciones

¿Contradicciones?. . .

Según el D.R.A.E.

Directorio

5. m. Guía en la que figuran las personas de un conjunto, con indicación de diversos datos de ellas, como su cargo, sus señas, su teléfono, etc.

Privacidad

1. f. Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.

Definiciones

¿Contradicciones?. . .

Según el D.R.A.E.

Directorio

5. m. Guía en la que figuran las personas de un conjunto, con indicación de diversos datos de ellas, como su cargo, sus señas, su teléfono, etc.

Privacidad

1. f. Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.

Privado

2. adj. Particular y personal de cada individuo.
3. adj. Que no es de propiedad pública o estatal, sino que pertenece a particulares.

Finalidad de las instituciones

lo que inicia el problema

Finalidad de las instituciones

lo que inicia el problema

Las instituciones públicas deben servir al público, por tanto deben. . .

Finalidad de las instituciones

lo que inicia el problema

Las instituciones públicas deben servir al público, por tanto deben. . .

- Ofrecer información sobre sí mismas.

Finalidad de las instituciones

lo que inicia el problema

Las instituciones públicas deben servir al público, por tanto deben. . .

- Ofrecer información sobre sí mismas.
- Ofrecer información sobre sus miembros.

Finalidad de las instituciones

lo que inicia el problema

Las instituciones públicas deben servir al público, por tanto deben. . .

- Ofrecer información sobre sí mismas.
- Ofrecer información sobre sus miembros.
- Colaborar entre ellas.

Necesidades de los usuarios

Necesidades de los usuarios

Los usuarios quieren

Necesidades de los usuarios

Los usuarios quieren

- Encontrar a los demás para comunicarse.

Necesidades de los usuarios

Los usuarios quieren

- Encontrar a los demás para comunicarse.
- Que otros, posibles colaboradores en sus proyectos, los puedan encontrar.

Necesidades de los usuarios

Los usuarios quieren

- Encontrar a los demás para comunicarse.
- Que otros, posibles colaboradores en sus proyectos, los puedan encontrar.

pero no quieren que

Necesidades de los usuarios

Los usuarios quieren

- Encontrar a los demás para comunicarse.
- Que otros, posibles colaboradores en sus proyectos, los puedan encontrar.

pero no quieren que

- se expongan sus datos

Cuestiones legales
que son parte del problema

Cuestiones legales
que son parte del problema

- El derecho a la intimidad de las personas.

Cuestiones legales
que son parte del problema

- El derecho a la intimidad de las personas.
  Las personas tienen derecho a reservarse información.

Cuestiones legales
que son parte del problema

- El derecho a la intimidad de las personas.
  Las personas tienen derecho a reservarse información.
- Los directorios accesibles por Internet se pueden considerar transferencias internacionales de datos personales.

Requisitos técnicos
que influyen en el problema

Requisitos técnicos
que influyen en el problema

- Se debe poder acceder al directorio directamente.

Requisitos técnicos
que influyen en el problema

- Se debe poder acceder al directorio directamente.
- La política se debe aplicar independientemente de la forma de acceso.

Requisitos técnicos
que influyen en el problema

- Se debe poder acceder al directorio directamente.
- La política se debe aplicar independientemente de la forma de acceso.
- Tratamiento diferente para

Requisitos técnicos
que influyen en el problema

- Se debe poder acceder al directorio directamente.
- La política se debe aplicar independientemente de la forma de acceso.
- Tratamiento diferente para
  - búsquedas internas

Requisitos técnicos
que influyen en el problema

- Se debe poder acceder al directorio directamente.
- La política se debe aplicar independientemente de la forma de acceso.
- Tratamiento diferente para
  - búsquedas internas
  - búsquedas externas

Requisitos técnicos
que influyen en el problema

- Se debe poder acceder al directorio directamente.
- La política se debe aplicar independientemente de la forma de acceso.
- Tratamiento diferente para
  - búsquedas internas
  - búsquedas externas
- Reducir los procesos de administración.

Distintas aproximaciones
para solucionar el problema

Distintas aproximaciones
para solucionar el problema

- La propuesta de los abogados

Distintas aproximaciones
para solucionar el problema

- La propuesta de los abogados

Eliminar el directorio

Distintas aproximaciones
para solucionar el problema

- La propuesta de los abogados

  Eliminar el directorio

- La propuesta de los usuarios

Distintas aproximaciones
para solucionar el problema

- La propuesta de los abogados

  Eliminar el directorio

- La propuesta de los usuarios

  Nada

Distintas aproximaciones
para solucionar el problema

- La propuesta de los abogados

  Eliminar el directorio

- La propuesta de los usuarios

  Nada, solo quieren *que funcione*

Distintas aproximaciones
para solucionar el problema

- La propuesta de los abogados

  Eliminar el directorio

- La propuesta de los usuarios

  Nada, solo quieren *que funcione*

- La propuesta de los técnicos

Distintas aproximaciones
para solucionar el problema

- La propuesta de los abogados

  Eliminar el directorio

- La propuesta de los usuarios

  Nada, solo quieren *que funcione*

- La propuesta de los técnicos

  Eliminar a los abogados

Puntos para encontrar una solución

sin tener que eliminar a nadie

Puntos para encontrar una solución
sin tener que eliminar a nadie

- Darle el control al usuario.

Puntos para encontrar una solución
sin tener que eliminar a nadie

- Darle el control al usuario.
- Que la organización pueda establecer la política.

Puntos para encontrar una solución
sin tener que eliminar a nadie

- Darle el control al usuario.
- Que la organización pueda establecer la política.
- Cumplir la ley.

Dos caras de la misma moneda

lado del usuario / lado del servidor

Dos caras de la misma moneda

lado del usuario / lado del servidor

- Lado del usuario

Dos caras de la misma moneda

lado del usuario / lado del servidor

- Lado del usuario
  El usuario debe poder controlar sus datos.

Dos caras de la misma moneda

lado del usuario / lado del servidor

- Lado del usuario
  El usuario debe poder controlar sus datos.
- Lado del servidor

Dos caras de la misma moneda

lado del usuario / lado del servidor

- Lado del usuario
  El usuario debe poder controlar sus datos.
- Lado del servidor
  La solución debe funcionar cualquiera que sea el interfaz.

El usuario manda en sus datos

El usuario manda en sus datos

Necesitamos:

El usuario manda en sus datos

Necesitamos:

- Interfaz para definir las preferencias del usuario.

El usuario manda en sus datos

Necesitamos:

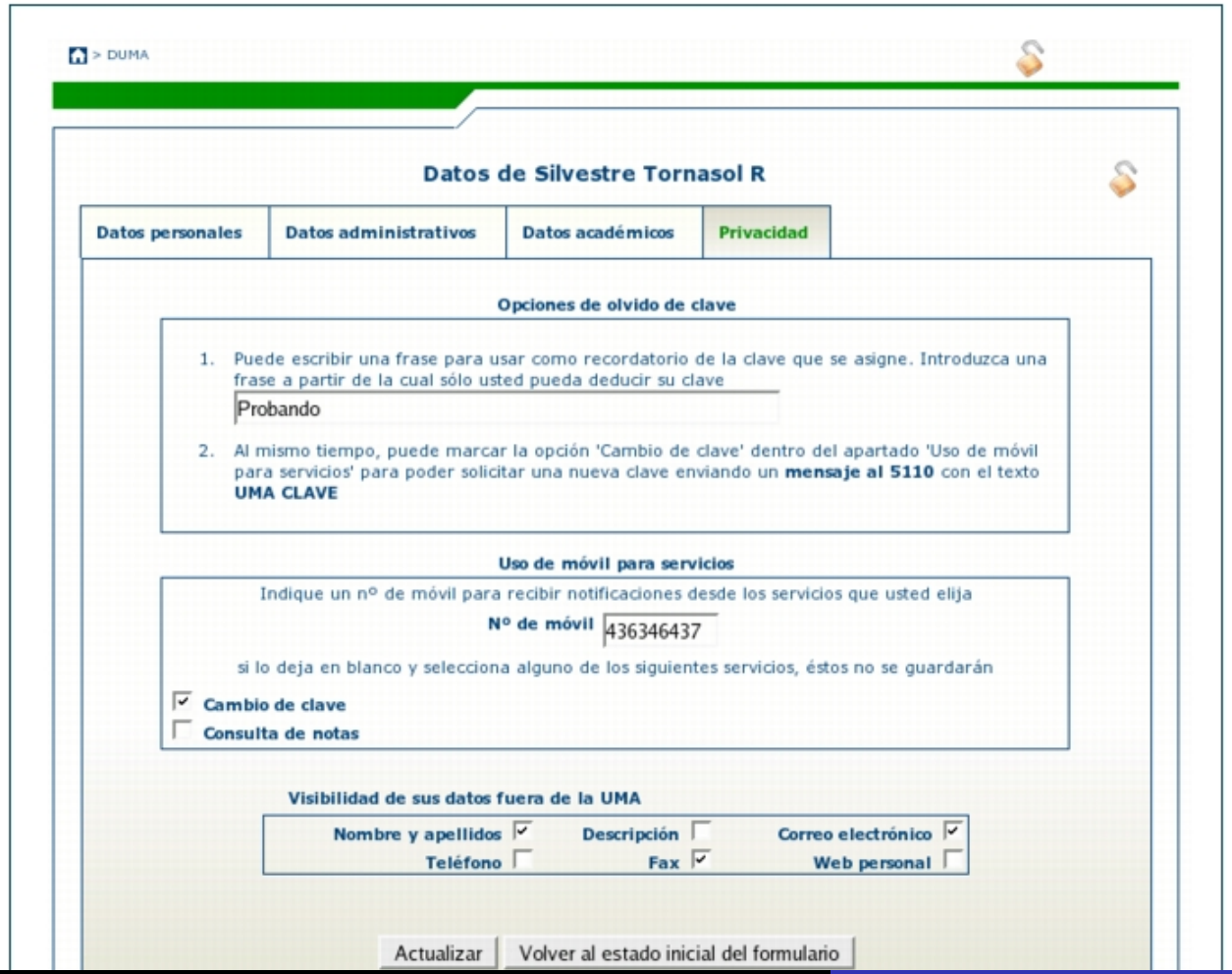
- Interfaz para definir las preferencias del usuario.
  Nos sabemos el camino

El usuario manda en sus datos

Necesitamos:

- Interfaz para definir las preferencias del usuario.
  Nos sabemos el camino un bonito formulario web.

El usuario manda en sus datos
con un bonito formulario web



El usuario manda en sus datos

Necesitamos:

- Interfaz para definir las preferencias del usuario.
  Nos sabemos el camino un bonito formulario web.
- Un atributo para guardar las preferencias en el directorio.

El usuario manda en sus datos

Necesitamos:

- Interfaz para definir las preferencias del usuario.
  Nos sabemos el camino un bonito formulario web.
- Un atributo para guardar las preferencias en el directorio.

irisUserPrivateAttribute

El usuario manda en sus datos

Necesitamos:

- Interfaz para definir las preferencias del usuario.
  Nos sabemos el camino un bonito formulario web.
- Un atributo para guardar las preferencias en el directorio.

schacUserPrivateAttribute

El usuario manda en sus datos

Necesitamos:

- Interfaz para definir las preferencias del usuario.
  Nos sabemos el camino un bonito formulario web.
- Un atributo para guardar las preferencias en el directorio.

schacUserPrivateAttribute

porque en Europa ha gustado la idea

La institución decide la política

La institución decide la política

- La política se debe aplicar independientemente del interfaz.

La institución decide la política

- La política se debe aplicar independientemente del interfaz.
  Se descarta el control a nivel de aplicación.

La institución decide la política

- La política se debe aplicar independientemente del interfaz.
  Se descarta el control a nivel de aplicación.
- Aplicación de la política a nivel del servidor.

La institución decide la política

- La política se debe aplicar independientemente del interfaz.
  Se descarta el control a nivel de aplicación.
- Aplicación de la política a nivel del servidor.
  Usando las ACL de OpenLDAP

Resumen

Resumen

- El usuario tiene el control de sus datos personales.

Resumen

- El usuario tiene el control de sus datos personales.
- La política se aplica en el servidor.

Resumen

- El usuario tiene el control de sus datos personales.
- La política se aplica en el servidor.
- Los abogados están contentos.

Resumen

- El usuario tiene el control de sus datos personales.
- La política se aplica en el servidor.
- Los abogados están contentos.
- La solución es sencilla.

Resumen

- El usuario tiene el control de sus datos personales.
- La política se aplica en el servidor.
- Los abogados están contentos.
- La solución es sencilla.
- y además

Resumen

- El usuario tiene el control de sus datos personales.
- La política se aplica en el servidor.
- Los abogados están contentos.
- La solución es sencilla.
- y además

FUNCIONA

Resumen

- El usuario tiene el control de sus datos personales.
- La política se aplica en el servidor.
- Los abogados están contentos.
- La solución es sencilla.
- y además

FUNCIONA

y estaremos encantados de enseñarlo a quien lo desee

Revelaremos nuestros atributos

aunque parcial y virtualmente

Revelaremos nuestros atributos

aunque parcial y virtualmente

Definiciones

LDAP, *Lightweigth Directory Access Protocol*

Fuente: Wikipedia.org (traducido del inglés)

Definiciones

LDAP, *Lightweigth Directory Access Protocol*

+ Protocolo de red que se usa para interrogar y modificar servicios de directorio que funcionan sobre TCP/IP.

Fuente: Wikipedia.org (traducido del inglés)

Definiciones

LDAP, *Lightweigth Directory Access Protocol*

- Protocolo de red que se usa para interrogar y modificar servicios de directorio que funcionan sobre TCP/IP.
- Normalmente, un directorio LDAP se ajusta al modelo X.500: un árbol de entradas cada una de las cuales consiste en un conjunto de atributos con nombre y valor.

Fuente: Wikipedia.org (traducido del inglés)

Definiciones

LDAP, *Lightweigth Directory Access Protocol*

- Protocolo de red que se usa para interrogar y modificar servicios de directorio que funcionan sobre TCP/IP.
- Normalmente, un directorio LDAP se ajusta al modelo X.500: un árbol de entradas cada una de las cuales consiste en un conjunto de atributos con nombre y valor.
- Un directorio LDAP refleja, la mayoría de las veces, divisiones políticas, geográficas y organizativas.

Fuente: Wikipedia.org (traducido del inglés)

Definiciones

LDAP, *Lightweigth Directory Access Protocol*

- Protocolo de red que se usa para interrogar y modificar servicios de directorio que funcionan sobre TCP/IP.
- Normalmente, un directorio LDAP se ajusta al modelo X.500: un árbol de entradas cada una de las cuales consiste en un conjunto de atributos con nombre y valor.
- Un directorio LDAP refleja, la mayoría de las veces, divisiones políticas, geográficas y organizativas.
- La versión actual es LDAPv3, que se define en el RFC 3377

Fuente: Wikipedia.org (traducido del inglés)

Definiciones

OpenLDAP

Fuente: Wikipedia.org (traducido del inglés)

Definiciones

OpenLDAP

+ Es una implementación libre de código abierto del protocolo LDAP.

Fuente: Wikipedia.org (traducido del inglés)

Definiciones

OpenLDAP

- Es una implementación libre de código abierto del protocolo LDAP.
- El programa lo desarrolla el Proyecto OpenLDAP y se distribuye con su propia licencia: *OpenLDAP Public License*.

Fuente: Wikipedia.org (traducido del inglés)

Definiciones

ACL, Access Control List *(Lista de control de acceso)*

Fuente: Wikipedia.org (traducido del inglés)

Definiciones

ACL, Access Control List *(Lista de control de acceso)*

+ Concepto de seguridad informática que se utiliza para hacer cumplir la separación de privilegios.

Fuente: Wikipedia.org (traducido del inglés)

Definiciones

ACL, Access Control List *(Lista de control de acceso)*

- Concepto de seguridad informática que se utiliza para hacer cumplir la separación de privilegios.
- Es un medio para determinar el derecho de acceso a un determinado objeto en función de ciertas características del proceso que realiza la petición, principalmente la identidad del usuario del proceso.

Fuente: Wikipedia.org (traducido del inglés)

Las ACL de OpenLDAP I

Política de privacidad para alumnos

irisUserPrivateAttribute puede contener el valor *all* o puede estar vacío, denegando o permitiendo el acceso a TODOS los atributos, definidos en *attrs*. En realidad, nuestra política actual para los datos personales de los alumnos, deniega el acceso a toda la entrada.

Denegar el acceso a todos los atributos

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(&(eduPersonAffiliation=student)
                  (irisUserPrivateAttribute=all))"
        attrs=entry
        by * none
```

Las ACL de OpenLDAP II

Política de privacidad para alumnos

Si un alumno elimina el valor de su irisUserPrivateAttribute, el sistema permitirá el acceso a la entrada y, de este modo, a los atributos permitidos por la política, para que se puedan mostrar.

Dar acceso a los atributos permitidos

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(eduPersonAffiliation=student)"
        attrs=entry,displayName,mail,telephoneNumber
        by * read
```

Las ACL de OpenLDAP III

Política de privacidad para PAS, PDI...

La institución puede decidir que una entrada no aparezca en las búsquedas. En ese caso, irisUserPrivateAttribute contiene el valor *entry*.

Denegando todo acceso

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(irisUserPrivateAttribute=entry)"
        by * none
```

Las ACL de OpenLDAP IV

Política de privacidad para PAS, PDI...

El usuario puede decidir qué atributos deben ocultarse de las búsquedas anónimas, escogidos de un conjunto definido por la política institucional. irisUserPrivateAttribute contendrá los nombres de dichos atributos. Si la búsqueda la realiza un usuario autenticado, los atributos se mostrarán.

Denegando acceso al número de teléfono

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(irisUserPrivateAttribute=telephoneNumber)"
        attrs=telephoneNumber
        by users read
        by * none
```

Las ACL de OpenLDAP V

Política de privacidad para PAS, PDI...

El usuario puede decidir ocultar todo el conjunto de atributos definido por la política institucional. En tal caso, irisUserPrivateAttribute contiene el valor *all*. Si la búsqueda la realiza un usuario autenticado, los atributos se mostrarán.

Denegando acceso a todos los atributos

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(irisUserPrivateAttribute=all)"
        attrs=mail,telephoneNumber,facsimileTelephoneNumber
        by users read
        by * none
```