|  |
| --- |
| Coordinación de informática |
| Desarrollo de Aplicaciones |
| Autenticación centralizada de usuarios |

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Estado** | **fecha** | **Observaciones** |
| 1.0 | Primera versión | 04/06/2015 | Incluye los dos escenarios y el diagrama de flujo |
| Autor: | Rubén Incostante | |
| Aprobó: |  | |

Contenido

[Requerimiento de acceso directo a una aplicación 3](#_Toc421210787)

[Solicitud 3](#_Toc421210788)

[Filtrado 3](#_Toc421210789)

[Lectura de cookie de usuario 4](#_Toc421210790)

[Persistencia de la url requerida en una cookie 4](#_Toc421210791)

[Acceso a la vista login de GestionAplicaciones 4](#_Toc421210792)

[Autenticación del usuario y persistencia de sus datos 4](#_Toc421210793)

[Lectura de la url 4](#_Toc421210794)

[Respuesta 4](#_Toc421210795)

[Acceso a AppCliente 4](#_Toc421210796)

[Persistencia del usuario en la sesión 4](#_Toc421210797)

[Requerimiento de acceso al portal de aplicaciones de la intranet 5](#_Toc421210798)

[Solicitud 5](#_Toc421210799)

[Filtrado 5](#_Toc421210800)

[Verificación de existencia de sesión 5](#_Toc421210801)

[Lectura de la url 5](#_Toc421210802)

[Acceso a la vista login de GestionAplicaciones 5](#_Toc421210803)

[Autenticación del usuario y persistencia de sus datos 5](#_Toc421210804)

[Persistencia del usuario en una cookie 5](#_Toc421210805)

[Respuesta 5](#_Toc421210806)

[Acceso a GestionAplicaciones 5](#_Toc421210807)

[Diagrama de flujo del procedimiento para ambos escenarios 5](#_Toc421210808)

Consideraciones

El presente documento describe el procedimiento de autenticación de usuarios en el nuevo contexto de aplicaciones para la intranet de la SAyDS.

Dicho contexto se compone del uso de JSF para la capa de aplicación y presentación y de la implementación de la interface javax.servlet.Filter para los filtros.

El alcance del procedimiento descrito comprende dos escenarios:

1. El requerimiento de acceso directamente a una aplicación
2. El requerimiento de acceso al panel de aplicaciones de la intranet

Ambos casos se describen a continuación y al final del documento se anexa un diagrama de flujo con la síntesis del proceso para los dos escenarios.

Se identificará a la aplicación requerida directamente con el nombre de AppCliente y al panel de aplicaciones de la intranet como GestionAplicaciones.

Los nombres de usuario que todas las aplicaciones utilizarán serán los correspondientes a los registrados en el Directorio Activo del dominio de la SAyDS, tanto para GestionAplicaciones como para todas las aplicaciones de la intranet.

La configuración de seguridad para usuarios será privativa de cada aplicación que las resolverá localmente. Asimismo, los atributos necesarios del usuario para cada aplicación.

# Requerimiento de acceso directo a una aplicación

## Solicitud

Desde un navegador se ingresa la url requiriendo AppCliente. El archivo de configuración de la aplicación (web.xml) deberá especificar el uso de la clase que implementa la interface javax.servlet.Filter y la ruta que filtrará, en este caso serán todas (/\*). Esto tendrá como consecuencia, que todo requerimiento a la url “[server]:[puerto]/AppCliente/” sea interceptada por el filtro.

Para el caso de aplicaciones desarrolladas con otra tecnología, deberá implementarse un filtro análogo.

## Filtrado

El filtro deberá permitir excepciones que no filtrará, rutas del tipo “.png”, “.ico”, “resources”, etc. Y no filtrará, especialmente, la ruta “[server]:[puerto]/AppCliente/login.[ extencion\_que\_corresponda]”, que será la vista que ofrecerá el formulario para el ingreso de las credenciales de usuario.

### Lectura de cookie de usuario

El método principal del filtro verificará si la ruta recibida está comprendida entre las excepciones, en cuyo caso redireccionará de la forma que corresponda.

Si la ruta debe ser interceptada, el filtro verificará la existencia de cookie de url, de existir, la borrará, a continuación buscará una cookie correspondiente al usuario que inició sesión.

Si existiera la cookie de usuario el filtro continuará con el redireccionamiento correspondiente.

### Persistencia de la url requerida en una cookie

Si no existiera la cookie del usuario, el filtro guarda la ruta requerida en una cookie de url y redirecciona a la vista de inicio de sesión de GestionAplicaciones (“[server]:[puerto]/ GestionAplicaciones/login.[extencion\_que\_corresponda]”).

### Acceso a la vista login de GestionAplicaciones

GestionAplicaciones tiene un filtro similar al descripto para AppCliente que validará si hay una sesión iniciada, en este caso no habrá ninguna, dado que esto ya se verificó con anterioridad, por tal motivo, el filtro redirige a la vista con el formulario para recibir las credenciales correspondientes.

### Autenticación del usuario y persistencia de sus datos

Una vez recibidas las credenciales de usuario GestionAplicaciones realiza la autenticación validando los datos recibidos por LDAP contra el Directorio Activo del dominio de la SAyDS, de ser correctos, obtiene los datos principales del usuario, los persiste en la sesión y guarda una cookie con el nombre encriptado del usuario. Luego redirecciona a la vista de bienvenida de GestionAplicaciones. Si los datos no fueran correctos se redireccionará a una vista de error.

### Lectura de la url

El requerimiento es filtrado pero esta vez ya existe una sesión iniciada por el usuario, de modo que el filtro verifica que no haya una cookie con la url requerida, cosa que sí habrá en el escenario descrito, por tal motivo, eliminará la cookie de la url y redireccionará a la url leída.

## Respuesta

### Acceso a AppCliente

La petición es nuevamente interceptada por el filtro de AppCliente, en este caso ya habrá un usuario persistido en una cookie, de modo que el filtro permitirá el acceso al recurso requerido y redireccionará a la vista de bienvenida.

### Persistencia del usuario en la sesión

Al acceder a la vista de bienvenida AppCliente, obtiene el usuario de la cookie, lo desencripta y lo persiste en memoria para proceder según la propia configuración local para dicho usuario.

# Requerimiento de acceso al portal de aplicaciones de la intranet

## Solicitud

Desde un navegador se ingresa la url requiriendo GestionAplicaciones. Como se detalló más arriba, esta aplicación también dispone de un filtro similar a la AppCliente con una similar configuración de su web.xml

## Filtrado

Como en el caso de la AppCliente, el filtro de GestionAplicaciones dispondrá de similares excepciones.

### Verificación de existencia de sesión

El Filtro interceptará el requerimiento y verificará la existencia de sesión iniciada.

### Lectura de la url

En caso de encontrar una sesión iniciada, el paso siguiente consiste en la búsqueda de una cookie con la url requerida, en este caso no la habrá, de modo que redireccionará a la vista de bienvenida de GestionAplicaciones.

### Acceso a la vista login de GestionAplicaciones

En caso de no haber una sesión iniciada, el filtro redireccionará al formulario de inicio de sesión de GestionAplicaciones (“[server]:[puerto]/ GestionAplicaciones/login.[extencion\_que\_corresponda]”).

### Autenticación del usuario y persistencia de sus datos

Una vez recibidas las credenciales de usuario GestionAplicaciones realiza la autenticación del modo que se indicó en la misma actividad del procedimiento para el escenario anterior.

### Persistencia del usuario en una cookie

En caso de ser autenticado el usuario, se persiste su nombre encriptado en una cookie y se procede a la lectura de la cookie de url que se explica más arriba.

## Respuesta

### Acceso a GestionAplicaciones

El Filtro volverá a interceptar la solicitud, pero como ya habrá una sesión iniciada, permitirá el acceso.

# Diagrama de flujo del procedimiento para ambos escenarios

