DISPOSICIONES PARA EL USO DE LA RED WI-FI

El Ersu de Sassari proporciona acceso a Internet a todos los estudiantes con una cama en sus residencias.
El servicio, exclusivamente inalámbrico, permite la movilidad de los terminales dentro de las distintas residencias (Via Coppino, Via Manzella, Via Rosello, Via Verona, Ex Brigata) utilizando las mismas credenciales proporcionadas por la Administración.

El primer acceso a la red inalámbrica constituirá una declaración de reconocimiento y aceptación total de estas Disposiciones de uso de la red Wi-Fi.

1. Normas generales

El incumplimiento de las Disposiciones conllevará medidas inmediatas que serán evaluadas en función de la gravedad de la actuación realizada y su reincidencia con la consiguiente desactivación permanente de los derechos de acceso.
Realizará un seguimiento de las actividades realizadas en la red con las credenciales del usuario. La Administración no accederá a dichos datos que, no obstante, podrán ponerse a disposición de las autoridades judiciales si éstas lo solicitan como consecuencia de actividades o comportamientos ilícitos.
Por último, se reitera que toda la responsabilidad civil y penal recae en los usuarios individuales de la red.
En caso de violación de estas Disposiciones, la Administración procederá a la revocatoria formal del usuario y pondrá la documentación relativa a disposición de la Autoridad Judicial si fuera necesario.

2. Derechos de acceso y credenciales

El acceso al servicio se realiza a través de una clave especial que permanece estrictamente personal y que se puede asociar a un solo dispositivo. La clave tiene la duración de todo el curso académico.
Es su responsabilidad mantener diligentemente sus credenciales de acceso a la red inalámbrica. Cualquier actividad no regular se atribuirá, dentro de los límites de la ley, al propietario.
Estas credenciales, al estar asociadas de forma única con su propietario, son estrictamente personales y, por lo tanto, intransferibles. En caso de ser transferidos a terceros, la responsabilidad de las actividades que realicen en la red recaerá en todo caso en el titular de las credenciales.
El usuario está obligado a informar inmediatamente de cualquier sospecha de robo, accidente, abuso o violación de la seguridad;
El Ersu de Sassari no asume ninguna responsabilidad en caso de uso indebido de las credenciales de acceso.
El uso de credenciales de acceso a los servicios informáticos se registrará en archivos especiales (Log) para los usos permitidos por la ley y por estas disposiciones. Si el usuario sospecha que sus credenciales han sido comprometidas, deberá comunicarlo sin demora al Sector de Alojamiento.
Las infraestructuras y servicios son propiedad del Ersu de Sassari. La misma administración podrá interrumpir, prohibir, bloquear el acceso y servicio, incluso a usuarios individuales, sin previo aviso y en cualquier momento.
Para permitir que todos puedan usar el servicio, cada usuario puede usar solo un dispositivo personal a la vez de su elección (PC, tableta, teléfono inteligente, etc.).

3. Normas de conducta

El usuario se compromete a respetar las siguientes normas de conducta:

a. Utilizar únicamente los recursos para los que está habilitado el servicio: es posible acceder libremente a Internet pero la Administración puede decidir en cualquier momento inhibir, a su discreción, los servicios que considere perjudiciales para un uso óptimo del ancho de banda disponible (programas para el intercambio de archivos, chats, etc.). La red debe utilizarse principalmente con fines educativos.

b. No intente acciones de escaneo de red o ataques de seguridad, ya que están expresamente prohibidos por la ley. Cabe señalar que para eventos como los mencionados anteriormente, es posible localizar el dispositivo y la cuenta que los originó.
c. No utilice la red de la Agencia para intercambiar material ilegal bajo ninguna circunstancia: el intercambio de material protegido por derechos de autor (por.MP3 ejemplo, películas DivX o DVD, software comercial, libros de texto, etc.) está expresamente prohibido por la ley y sujeto a sanciones penales. En caso de detección de actuaciones ilícitas, se realizará un informe a la Autoridad Judicial.
d. También está prohibido:
    - difundir imágenes, datos u otro material con contenido pornográfico, obsceno, blasfemo, racista, difamatorio y ofensivo;
    - utilizar la Red de Datos de Ersu y los servicios que ofrece con fines comerciales y de propaganda política o electoral;
    - destruir o intentar destruir, dañar o intentar dañar, interceptar o intentar interceptar o acceder o intentar acceder sin autorización al correo electrónico o datos de otros usuarios o terceros, usar, interceptar o difundir o intentar interceptar o difundir contraseñas o códigos de acceso o claves criptográficas de otros usuarios o terceros, y en general cometer o intentar cometer actividades que violen la confidencialidad de otros usuarios o terceros, según lo protegido por las regulaciones civiles, penales y administrativas aplicables;
    - transferir grandes cantidades de datos, si no es realmente necesario;
    - no configurar puntos de acceso a la red mediante el uso de dispositivos personales;
e. No configure manualmente los ajustes de red de su dispositivo, la infraestructura de acceso asigna automáticamente los parámetros necesarios para el uso del servicio. La configuración manuales de los parámetros puede provocar un mal funcionamiento de la conexión para uno mismo y para otros usuarios.
f. No utilice la red inalámbrica para realizar comunicaciones directas entre usuarios: el ancho de banda disponible no es ilimitado, manténgalo ocupado para comunicaciones duraderas limita la capacidad de otros usuarios para acceder a los servicios de manera más efectiva.
g. El usuario debe equipar su dispositivo con protecciones adecuadas contra virus u otro tipo de intrusiones. La Entidad no asume ninguna responsabilidad por los datos contenidos en los dispositivos de los usuarios del servicio. En el caso de un ataque por un virus informático u otro tipo de ataque, el usuario no podrá tomar represalias contra la Entidad de ninguna manera. Por lo tanto, se invita a los usuarios a instalar un software antivirus eficiente y actualizado y un firewall personal configurado correctamente en sus equipos.