SEGURIDAD TIC EN EL CENTRO

Tema 2

Índice

1. Introducción....3
2. Seguridad física....5
2.1. Recomendaciones....6
2.2. Normativa y documentos de interés....8
3. Seguridad lógica....9
3.1. Contraseñas seguras....11
3.2. Recomendaciones de seguridad para los usuarios de la red del centro....14
3.3. Cortafuegos....15
3.3.1 Cortafuegos en Lliurex....17
3.4 Copias de seguridad....18
3.4.1 Copias de seguridad en Lliurex....19
4. Amenazas y vulnerabilidades....21
4.1 Tipos de malware....21
4.2. Métodos de protección....23
4.2.1 Malware en Lliurex....24
4.2.2 Aplicaciones antivirus....24
5. Red interna y wifi....25
5.1. Configuración segura....26
5.2. Mantenimiento seguro de la red wifi....28
5.3. Buen uso de la red....29
5.4. Freeradius....29
6. Bibliografía....31
7. Autoría....31
Actividades....33

1. Introducción

El incremento exponencial del uso de las nuevas tecnologías en nuestros centros, y la cada vez mayor dependencia de los sistemas de información que todos tenemos, motivan que la seguridad de la información tenga un papel básico en nuestro día a día: en la actualidad, nadie cuestiona la importancia de la **disponibilidad** de los sistemas de información, y de la **integridad y confidencialidad** de los datos que estos gestionan. No tenemos más que pensar en las actividades que a diario desarrollamos conectados a la red: desde consultas o movimientos bancarios, hasta compartición de información por múltiples canales (páginas web, mensajería instantánea, telefonía...) o incluso relaciones personales y profesionales. Por supuesto, al igual que en nuestro entorno 'real' nos preocupa la seguridad, debe preocuparnos en el entorno virtual de Internet.

Al hablar de seguridad, son tres los pilares sobre los que se basa ésta:

- **Disponibilidad**: Debemos tener garantías de que la información va a estar disponible en el momento en que se necesita.
- **Integridad**: Debemos tener garantías de que la información es exacta, y de que está protegida frente a alteraciones o pérdidas.
- **Confidencialidad**: Debemos tener garantías de que solo las personas autorizadas disponen de acceso a la información

Obviamente, garantizar la seguridad de la información es un aspecto crítico para todos nosotros y para las organizaciones que nos prestan servicios (empresas, administraciones, públicas etc.), sin importar su tamaño o su sector de actividad; la importancia de la seguridad es especialmente relevante en aquellos entornos en los que se manejan datos especialmente protegidos por leyes como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD). Así, la seguridad de la información no es solo un tema técnico, sino también un tema legal, con aspectos perfectamente regulados y que, más allá de decisiones, concienciaciones o preferencias particulares, todos estamos obligados a cumplir.

¿Conoces el equipamiento TIC de tu centro?

Son varias las instrucciones de servicio donde se habla de un responsable de la electrónica de red:

“La manipulación de la electrónica de red que proporciona acceso a Internet en la secretaría y las aulas de los centros deberá estar controlada por un responsable para evitar cualquier manipulación

ajena, quien llevará un registro con el histórico de actuaciones que se realizan sobre la electrónica y quien las realiza (visitas de técnicos, cambio de latiguillos, ...) Se recomienda que la electrónica de red se ubique en un espacio dedicado, tal como un armario de comunicaciones, al que llegue red eléctrica para alimentación de los equipos. Dicho espacio se recomienda que disponga de acceso controlado por el responsable, y que permanezca cerrado."

- INSTRUCCIÓN DE SERVICIO NÚM. 3/2010
- INSTRUCCIÓN DE SERVICIO NUM 5/2012

¿Conocemos cual es la electrónica de red? ¿Conocemos el equipamiento TIC ?

Para poder desempeñar mejor nuestro cargo, debemos familiarizarnos con las infraestructuras y equipamiento del centro, y con algunos conceptos técnicos que nos van a resultar útiles.

En el curso inicial para Coordinadores TIC ya vimos que todos los centros docentes cuentan con :

- una red interna de centro
- acceso a internet
- telefonía IP
- dotación informática

En él estudiamos las características básicas de la dotación de un centro educativo, en esta ocasión vamos a seguir formándonos en la seguridad informática, el área relacionada con la informática que se enfoca en la protección de la infraestructura y todo lo relacionado con esta y, especialmente, la información contenida en las redes de ordenadores.

La ciberseguridad comprende software, hardware, redes y todo lo que signifique un riesgo si información confidencial llega a manos de otras personas. Por tanto consiste en asegurar que los recursos del sistema de información se utilizan correctamente y que el acceso a la información allí contenida así como su modificación solo sea posible a las personas autorizadas.

El estado de la seguridad en la mayoría de los centros educativos refleja el desconocimiento que existe sobre las graves deficiencias de seguridad relacionadas con el uso de las nuevas tecnologías. Simplemente no se percibe la sensación de riesgo. Aunque, por un lado, la seguridad parece deseable, al mismo tiempo no es un asunto que parezca prioritario a pesar de la creciente dependencia en las TIC. El objetivo de este tema es que vayamos tomando conciencia de esta problemática y aprender a mantener seguros nuestros centros educativos.

2. Seguridad física

Se refiere a todos aquellos mecanismos --generalmente de prevención y detección-- destinados a proteger físicamente cualquier recurso de nuestro Centro. Estos recursos son desde un simple teclado hasta un *backup* con toda la información que hay en el sistema.

La posibilidad de acceder físicamente a una máquina hace inútiles casi todas las medidas de seguridad que hayamos aplicado sobre ella. Hemos de pensar que si se puede llegar con total libertad hasta un ordenador, por ejemplo, se podría abrir y sustraer el disco duro; sin necesidad de privilegios en el sistema, sin importar la robustez de nuestros cortafuegos, sin ni siquiera una clave de usuario, el atacante podría seguramente modificar la información almacenada, destruirla o simplemente leerla.

Incluso sin llegar al extremo de desmontar la máquina, que quizás resulte algo exagerado en nuestros centros, la persona que accede al equipo puede arrancar una versión diferente del sistema operativo sin llamar mucho la atención. Le resultará fácil utilizar un disco de arranque, montar los discos duros de la máquina y extraer de ellos la información deseada.

Visto esto, parece claro que cierta seguridad física es necesaria para garantizar la seguridad global de la red y los sistemas conectados a ella; evidentemente el nivel de seguridad física depende

completamente del entorno donde se ubiquen los equipos, materiales o recursos a proteger. Mientras que parte de los equipos estarán bien protegidos, por ejemplo los servidores de un departamento o los ordenadores de los despachos, otros muchos estarán en lugares de acceso público, como aulas de informática; es justamente sobre estos últimos sobre los que debemos extremar las precauciones.

2.1. Recomendaciones

Empecemos por tanto por lo más obvio, la disposición de los equipos en el aula de informática, el dificultar el que puedan ser manipulados incrementa la seguridad, así por ejemplo nos podemos hacer preguntas como estas ¿no hay otra distribución posible para los equipos en el aula?, ¿no nos pueden robar una memoria RAM o una tarjeta gráfica?, ¿no se nos puede perder todo el trabajo de un grupo por un corte eléctrico inoportuno?, etc. Por eso, cuando sea posible podemos seguir estas sencillas indicaciones:

1. Distribuir los ordenadores del aula de informática de modo que el profesor pueda tener todas las pantallas a la vista desde un punto de la sala, pensando en la mayor comodidad para impartir las clases.
2. Conducir los cables por detrás de las mesas, fuera de zonas de paso, sillas, etc. También podemos utilizar accesorios organizadores de cables.
3. Situar los dispositivos de red (ej. switches, routers y puntos de acceso wifi) en armarios de comunicaciones cerrados o al menos fuera del alcance de los usuarios.
4. Utilizar sistemas de protección eléctrica frente a picos de tensión (ej. regletas con protección). Trabajar con ordenadores implica trabajar con electricidad por lo tanto este es uno de los principales aspectos a considerar en la seguridad física. Si sufrimos frecuentes microcortes eléctricos, tenemos equipos especialmente sensibles, o hay maquinaria industrial que pueda afectar a la red (como en algunos centros de F.P.), podemos utilizar sistemas de alimentación ininterrumpida, SAI, en inglés uninterruptible power supply (UPS). Se trata de un dispositivo que gracias a sus baterías puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados. Otra de las funciones importantes que tiene es la de mejorar la calidad de la energía eléctrica que llega a los equipos, filtrando subidas y bajadas de tensión, por tanto su uso es especialmente recomendado en equipos que tengan una función importante en la red, como puedan ser los servidores.
5. Colocar candados en las cajas/torres de los ordenadores para evitar que se pueda acceder a su interior.

6. Instalar cables de seguridad o candados antirrobo en las pantallas u otros elementos de valor, fijándolos a la mesa, pared, etc.
7. Reservar un armario con llave para guardar los componentes de repuesto, por ej. cables de red, los discos CD y DVD, las licencias y manuales del software del aula (drivers y aplicaciones), así como los documentos con la estructura y configuración de la red y los ordenadores.

Si la mayoría de ordenadores del centro están en red se pueden conectar a Internet, compartir archivos entre sí, imprimir en la misma impresora, etc. Sin embargo, si no tenemos un mínimo cuidado en la configuración de la red, podemos dejar fácil acceso a información sensible como por ejemplo notas, teléfonos de los profesores, etc.

> “Los centros educativos disponen de dos líneas de acceso: la conexión de Secretaría y la conexión de Aula. La conexión de Secretaría se utiliza para tareas administrativas y únicamente se conectan los equipos de administración y del equipo directivo. La conexión de Aula se utiliza para tareas docentes y conectándose pues el equipamiento de Sala de Profesorado, Aulas de Informática, Departamentos, Aulario...

Así pues, lo ideal es separar la red de nuestros centros entre los ordenadores de gestión (secretaría, dirección) y los de las aulas (aulas ordinarias, aulas de informática) de modo que no sea posible que se comuniquen entre sí.

Recordad que hay dos instrucciones de servicio donde se recogen todas las medidas de seguridad a adoptar son la INSTRUCCIÓN DE SERVICIO NÚM. 3/2010 i la INSTRUCCIÓN DE SERVICIO NUM 5/2012 en las que cabe hacer especial mención a la separación de las redes de secretaría y de aulas. Esta es una medida física de especial importancia.

Todas estas sugerencias pueden ser adaptadas a cada centro educativo según sus posibilidades. ¿Se os ocurre alguna más? Os invitamos a compartirlas en el foro del curso.

2.2. Normativa y documentos de interés

Recopilación de la Normativa y Documentación relativa al uso y gestión de las comunicaciones de los centros educativos.

Instrucciones de Servicio IS 5/2012

Para el correcto uso y gestión de las líneas de datos de los centros educativos
http://www.ceice.gva.es/documents/161862998/163024947/Instrucción+servicio+5_2012+C.pdf

Instrucción Técnica - No 1/2011

Instalación de Telecomunicaciones en los Centros Escolares
http://www.ceice.gva.es/documents/161863110/163204930/instruccion2011_cas.pdf

Más Información

Las comunicaciones en los centros
http://mestreacasa.gva.es/c/document_library/get_file?folderId=500005015860&name=DLFE-262030.pdf

Guías

Guía para configurar la red en un equipo con LliureX en Secretaría
http://mestreacasa.gva.es/c/document_library/get_file?folderId=500002443671&name=DLFE-261988.pdf

3. Seguridad lógica.

La mayoría de los daños que puede sufrir un sistema informático no será unicamente los medios físicos sino contra la información almacenada y procesada. El activo más importante que se posee es la información y por tanto deben existir técnicas más allá de la seguridad física que la aseguren. Estas técnicas las brinda la seguridad lógica.

La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para ello.

Los objetivos que se plantean serán:

- Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no les correspondan.
- Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto analizando periódicamente los mismos.

Un aspecto crítico en la seguridad de la red de nuestro centro es que cada usuario tenga los privilegios correctamente asignados de manera que no pueda acceder a información para la cual no tiene permiso.

> “ Ya hemos visto cómo securizar nuestra red a nivel físico, en cuanto a software, LLiurex nos ofrece gestión de usuarios sencilla a través de su herramienta Llum que nos permitirá asignar a cada usuario de la red únicamente los permisos que sean necesarios y evitar de esta manera accesos indebidos a archivos.

Es conveniente que los usuarios sean identificados y autenticados una sola vez, pudiendo a partir de ahí acceder a todas las aplicaciones y datos que su perfil permita, ya sea en local o remoto. Esto se denomina SINGLE LOGIN. Una de las posibles técnicas para implementar esta única identificación sería la utilización de servidores de autenticación sobre el que se identifican los usuarios y que se encarga luego de autenticar al usuario sobre los restantes equipos. Este servidor no tiene que ser necesariamente un solo equipo y puede tener sus funciones distribuidas geográficamente de acuerdo a los requerimientos de carga de tarea. Toda esta configuración ya está implementada en el modelo de centro Lliurex con lo cual a nivel técnico lo tenemos resuelto.

> La seguridad informática se basa en gran medida en la efectiva administración de los permisos de acceso a los recursos informáticos basados en la identificación, autenticación y autorización de los accesos. Se conseja encarecidamente **no utilizar usuarios genéricos para acceder a los equipos de los centros.**

Para ampliar:

- Gestión de grupos de red en Lliurex
- Gestión de usuarios de red en Lliurex
- Gestión de usuarios de red en Windows

3.1. Contraseñas seguras

El nombre de usuario

Desde el punto de vista del sistema, el nombre de usuario es la respuesta a la pregunta "¿Quién es usted?". Como tal, los nombres de usuarios tienen un requerimiento principal — deben ser únicos.

Contraseñas seguras

Si el nombre de usuario responde a la pregunta "¿Quién es usted?", la contraseña es la respuesta a la pregunta que inevitablemente sigue: "¡Demuéstralo!".

En términos prácticos, una contraseña proporciona una forma de probar la autenticidad de la persona que dice poseer ese nombre de usuario. La efectividad de un esquema basado en contraseñas recae en gran parte sobre varios aspectos:

- La confidencialidad de la contraseña
- La resistencia de adivinar la contraseña
- La resistencia de la contraseña ante un ataque de fuerza bruta

Las contraseñas que efectivamente toman en cuenta estos problemas se conocen como contraseñas robustas, mientras que aquellas que no, se les llama débiles. Es importante para la

seguridad de los centros crear contraseñas robustas. Hay dos opciones disponibles para reforzar el uso de contraseñas robustas:

- El administrador puede crear contraseñas para todos los usuarios.
- El administrador puede dejar que los usuarios creen sus propias contraseñas, a la vez que se verifica que las contraseñas sean lo suficientemente robustas.

La necesidad de mantener secretas las contraseñas debería ser una parte arraigada en los hábitos de todos usuarios. Sin embargo, este punto se pierde con frecuencia, es de vital importancia educarlos para que puedan entender que sus contraseñas se deberían mantener secretas.

Las contraseñas deberían ser tan difíciles de adivinar como sea posible. Una contraseña robusta es aquella que un atacante no podrá adivinar, aun si el atacante conoce bien al usuario.

Para un atacante una contraseña segura debe parecerse a una cadena aleatoria de caracteres, puede conseguir que su contraseña sea segura siguiendo los siguientes criterios:

- **Que no sea corta,** cada carácter que agrega a su contraseña aumenta exponencialmente el grado de protección que esta ofrece, las contraseñas deben contener un mínimo de 8 caracteres lo ideal es que contengan 14 o más, muchos sistemas también admiten el uso de la barra espaciadora de modo que se pueden crear contraseñas de varias palabras (una frase codificada) por lo general una frase codificada resulta más fácil de recordar y más difícil de adivinar que una contraseña simple.
- **Combina letras, números y símbolos**, cuantos más diversos sean los tipos de caracteres más difícil será adivinarla.
- **Cuantos menos tipos de caracteres haya en la contraseña más larga deberá ser esta**. Una contraseña de 15 caracteres formada únicamente por letras y números es unas 33000 veces más segura que una de 8 caracteres compuesta por caracteres de todo tipo. Si la contraseña no puede tener símbolos deberá ser considerablemente más larga para conseguir el mismo grado de protección. Una contraseña ideal combinaría una mayor longitud y distintos tipos de símbolos.
- **Utiliza todo tipo de teclas**, no limitarse a los caracteres más comunes. Los símbolos que necesitan que se presione la tecla mayúscula junto con un número son muy habituales. La contraseña será mucho más segura si eliges entre todos los símbolos del teclado incluidos los símbolos de puntuación así como los exclusivos del idioma.
- **Utiliza palabras y frases que te resulten fáciles de recordar pero que a otras personas les sea difícil de adivinar**. La manera más sencilla de recordar las contraseñas y frases

codificadas consiste en anotarlas. No hay nada malo en anotar las contraseñas si bien estas anotaciones deben estar debidamente protegidas para que resulten seguras y eficaces.

- **Utiliza varias contraseñas para distintos entornos**, si alguno de los equipos o sistemas en línea que utilizan esta contraseña queda expuesto, toda la información protegida también estará en peligro.

Algunas estrategias que deben evitarse son:

- **Incluir secuencias y caracteres repetidos**, cadenas como 12345678, 22222222, abcdefg o el uso de letras adyacentes en el teclado no ayudan a crear contraseñas seguras.
- **Utilizar sustituciones de letras por símbolos** o números similares por ejemplo la i por el 1, la a por la @, o la o por el 0. Estas sustituciones pueden ser eficaces cuando se combinan con otras medidas, con una mayor longitud, errores ortográficos voluntarios, variaciones entre mayúsculas y minúsculas.
- **Utilizar el nombre de inicio de sesión**, cualquier parte del nombre, fecha de nacimiento o datos similares propios o de tus familiares constituye una mala elección.
- **Utilizar palabras del diccionario** de ningún idioma los delincuentes emplean herramientas capaces de descifrar rápidamente contraseñas basadas en palabras de distintos diccionarios que también abarcan palabras inversas, errores ortográficos comunes y sustituciones, esto incluye todo tipo de blasfemias.

Opción de contraseña en blanco: Una contraseña en blanco en su cuenta es más segura que una contraseña poco segura como 1234, puedes optar por usar contraseñas en blanco en la cuenta del equipo si se cumplen estos criterios:

- Tiene solo un equipo o bien tiene varios pero no necesita obtener acceso a la información de un equipo desde los otros
- El equipo es físicamente seguro (se confía en todas las personas que tienen acceso físico al equipo).

No siempre es buena idea usar una contraseña en blanco, por ejemplo es probable que un equipo portátil no sea físicamente seguro.

> “ Cuida tus contraseñas y frases codificadas tanto como la información que protegen, no la reveles a nadie, protege las contraseñas registradas, no las facilites nunca por correo electrónico, cambia tus contraseñas con regularidad y no las escribas en equipos que no controlas.

3.2. Recomendaciones de seguridad para los usuarios de la red del centro.

Con frecuencia la parte más complicada de una política de seguridad es concienciar a los usuarios de la necesidad de medidas básicas de prevención contra ataques. Demasiados usuarios opinan que las historias de crackers que atacan ordenadores solo suceden en las películas o en organizaciones militares de alta seguridad; nada más lejos de la realidad. Estas son algunas normas que el coordinador TIC puede divulgar entre los miembros del centro para ir concienciando de su importancia.

- Ya hemos visto cómo crear una contraseña aceptable y lo importante de mantenerla privada, además es muy recomendable que **nunca, bajo ningún concepto, instalar o ejecutar software que no provenga de fuentes fiables**; hay que prestar atención especial a programas que nos envíen por correo, ya que se puede tratar de programas trampa que, desde borrar todos nuestros ficheros, a enviar por correo una copia del archivo de contraseñas, pueden hacer cualquier cosa: imaginemos que un `amigo' nos envía un juego a través de cualquier medio y nosotros lo ejecutamos. Ese programa puede hacer algo tan simple como rm -rf $HOME/* (borrando todos los archivos del usuario) sin que nosotros nos demos cuenta, con las consecuencias que esta orden implica.
- Por tanto debemos **educar en la desconfianza** de cualquier correo electrónico, llamada telefónica o mensaje de otro tipo que nos indique realizar una determinada actividad en el sistema, especialmente cambiar la clave o ejecutar cierta orden; con frecuencia, un usuario se convierte en cómplice involuntario de un atacante.
- Un último consejo, **cualquier actividad sospechosa que detectemos, aunque no nos implique directamente a nosotros, ha de ser notificada**. Esta notificación, a ser posible, no se ha de realizar por correo electrónico (un atacante puede eliminar ese mail), sino en persona o por teléfono. En muchas ocasiones, cuando un usuario nota un comportamiento extraño en el sistema, no notifica nada pensando que el administrador ya se ha enterado del suceso, o por miedo a quedar en ridículo (quizás que lo que nosotros consideramos `extraño' resulta ser algo completamente normal); esta situación es errónea: si se trata de una falsa alarma, mucho mejor, pero… ¿y si no lo es?

3.3. Cortafuegos

Uno de los elementos de seguridad a nivel de software más interesantes y sencillos de implementar es un cortafuegos (firewall). El cortafuegos o Firewall es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado permitiendo al mismo tiempo comunicaciones autorizadas

Los cortafuegos también pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección como ya hemos visto.

VENTAJAS de un cortafuegos:

- Protección de intrusiones, el acceso a ciertos segmentos de la red sólo se permite a máquinas autorizadas de otros segmentos o de Internet.
- Protección de la información privada: permite definir distintos niveles de acceso a la información de manera que cada grupo de usuarios definido tenga solo acceso a los servicios e información que les son estrictamente necesarios.
- Optimización de acceso: Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa.
- LIMITACIONES de un cortafuegos: Cualquier tipo de ataque informático que use tráfico aceptado por el cortafuegos o que sencillamente no use la red seguirá constituyendo una amenaza.

Hay 2 políticas básicas en la configuración de un cortafuegos que cambian radicalmente la filosofía de la seguridad de la información:

- Política restrictiva: se deniega todo el tráfico excepto el que está explícitamente permitido por tanto hay que habilitar expresamente los servicios que se necesiten.
- Política permisiva: se permite todo el tráfico excepto el que está denegado. Cada servicio potencialmente peligroso necesitará ser aislado mientras que el resto de tráfico no será filtrado.

La política restrictiva es la más segura ya que tiene control para no permitir tráfico peligroso. Sin embargo la política permisiva es posible que no haya contemplado tráfico peligroso y sea aceptado por omisión. No es recomendable tener más de un cortafuegos ejecutándose simultáneamente en la misma máquina.

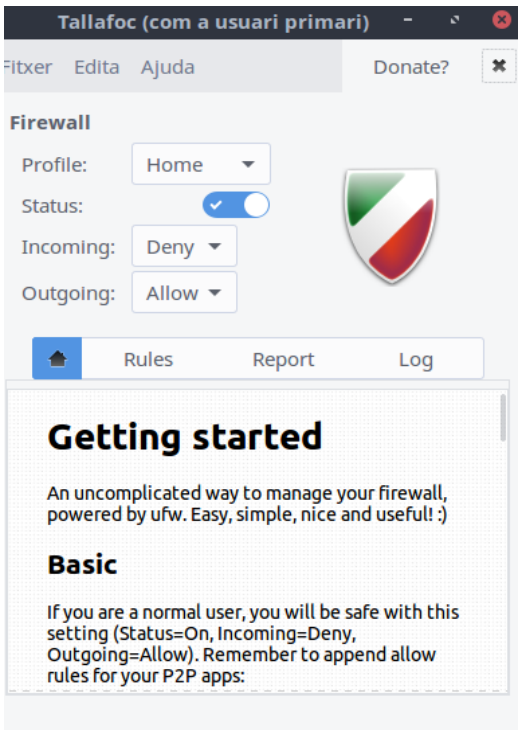
Algunos de los cortafuegos más conocidos son:

- Firestarter
- ZoneAlarm
- Uncomplicated Firewall
- Gufw
- ipfw
- PF (software)
- Forefront TMG

> Con el fin de garantizar una navegación segura, se ha implantado un sistema de filtrado y seguridad de contenidos en la red de Consellería de manera que se impide el acceso a contenidos no aptos para el alumnado, se analiza la presencia de virus, malware... y se protege de ataques externos.

3.3.1 Cortafuegos en Lliurex

En el menú Ajustes podéis encontrar el Cortafuegos de Lliurex, nos pedirá la contraseña de superusuario para ejecutarse. Veremos la siguiente ventana:



Por defecto viene desactivado, si lo queremos activar pulsamos en "Estado" y comprobamos que las siguientes opciones están activadas:

- Perfil: casa
- Entrante: denegar
- Saliente: permitir

Con eso ya tenemos la configuración básica activada. La configuración avanzada es muy sencilla, si quieres saber cómo gestionarla visita este enlace.

> Si disponemos de un modelo de aula o de centro también podemos hacer uso de Lliurex Guard para filtrar contenido desde el servidor.

3.4 Copias de seguridad

Más vale prevenir que lamentar y ya no solo en casos en que haya datos de carácter personal sino para cualquier información sensible que manejemos en el centro. El uso de discos duros externos o sistemas de backup, nos garantiza que al menos siempre habrá un sistema al que recurrir en caso de pérdida de datos.

¿Qué pasaría si de repente toda la información que almacenamos (documentos, fotografías, contraseñas, mensajes de correo electrónico, etc) desapareciera? Sin duda, sería una auténtica tragedia.

Debemos entender que los ordenadores no son inmunes a las averías del disco interno, virus o incluso eliminaciones “accidentales”. Por eso, ser conscientes de la importancia de realizar una copia de seguridad o “backup” periódicamente, nos ayudará a prevenir la pérdida de datos.

Algunos aspectos claves a tener en cuenta son:

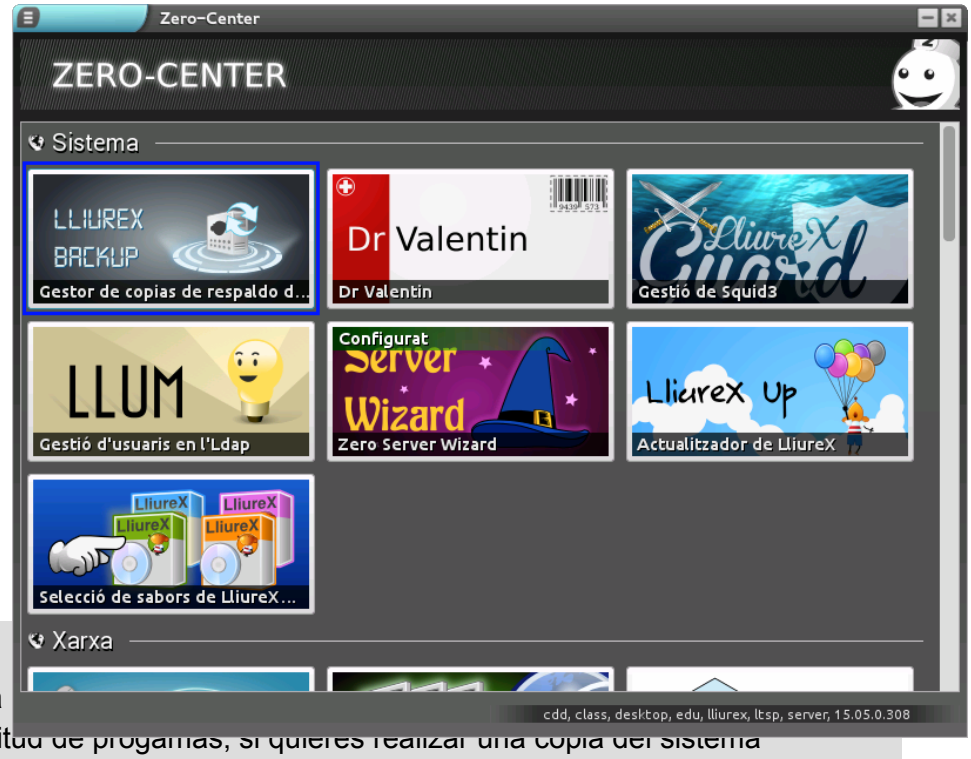
1. **Integridad** en los datos. Debe asegurarse de que los datos, de los que va a hacer una copia de seguridad, no están dañados ni incompletos.
2. **Cobertura**. Ante la pregunta “¿de qué debemos hacer backup?“, cuestione cuáles serían los datos que podría echar más en falta en caso de pérdida.
3. **Frecuencia**. Realice copias de seguridad con la misma frecuencia con la que trabaja en su ordenador. Si todos los días modifica sus datos pero tan sólo programa una copia de seguridad al mes, en caso de pérdida antes de la fecha del backup, todas las modificaciones se perderán.
4. **Separación**. Tras realizar las copias es importante que no todas se guarden en el mismo lugar. Tenemos que archivar y distribuir las copias en lugares distintos para que en caso de pérdida, robo o catástrofe natural, podamos recuperar, como mínimo, una de las copias.
5. **Historial**. No guarde únicamente el último backup que hizo, sino también los anteriores a este, al menos durante un tiempo prudencial. Por ejemplo, si hoy se da cuenta de que ha desaparecido un archivo importante y al restaurar el backup de ayer este no está, podrá retroceder en el tiempo hasta encontrarlo.
6. **Pruebas**. Llegados a este punto, en el que hemos realizado copias de seguridad de todo lo necesario, con frecuencia periódica y guardado en distintos lugares, debemos comprobar que realmente dichas copias funcionan correctamente. Para ello, es necesario hacer pruebas de restauración imaginándose que necesita un archivo determinado y comprobando que realmente se ha guardado.

7. **Seguridad**. Proteja los datos del backup de la misma forma que lo hace con los datos originales en su ordenador. No sirve de nada proteger nuestro ordenador con las mejores medidas de seguridad si mientras tanto nuestros datos del backup son fácilmente accesibles.

3.4.1 Copias de seguridad en Lliurex

Para hacer copias automatizadas de archivos de usuario podemos utilizar la herramienta que viene instalada por defecto en Lliurex llamada *Déjà Dup* la puedes lanzar desde el buscador de aplicaciones escribiendo “copia...” o desde el menú Ajustes – Copias de seguridad. Es una herramienta sencilla que permitirá tener a salvo todos tus documentos, si se desea profundizar en su uso puedes visitar el siguiente tutorial.

LliureX en el ámbito del modelo de aula/centro nos ofrece en el servidor la herramienta LliureX Backup, la cual permite realizar copias de respaldo de los archivos y servicios del aula. Concretamente, los servicios agrupados son: hostname, red, dnsmasq, samba, CUPS (configuración, impresoras y PPD), Apache (configuración del servicio, /var/www y todos los easy-sites), MySQL (password de root y volcado de la base de datos completa). Más información…



> “Para
> multitud de progamas, si quieres realizar una copia del sistema
> completo puedes utilizar el siguiente manual o este otro.

4. Amenazas y vulnerabilidades

Las amenazas y las vulnerabilidades son el objetivo central de los ataques. Una amenaza a la ciberseguridad es la posibilidad de que ocurra un evento nocivo, como un ataque. Una vulnerabilidad es una debilidad que hace que un objetivo sea susceptible a un ataque. Un ataque es una explotación deliberada de una debilidad detectada. Los delincuentes informáticos pueden tener diferentes motivaciones para seleccionar un objetivo de un ataque. Los delincuentes cibernéticos tienen éxito al buscar e identificar continuamente los sistemas con vulnerabilidades evidentes. Las víctimas comunes incluyen sistemas sin parches o sistemas que no cuentan con detección de virus y de correo no deseado.

Vamos a examinar los ataques más comunes a la ciberseguridad. Debemos saber cómo funciona cada ataque, lo que aprovecha y cómo nos puede afectar para poder proteger nuestro centro. Empezaremos explicando la amenaza de malware y de código malicioso, y luego explicaremos los tipos de trucos involucrados en la ingeniería social.

4.1 Tipos de malware

El malware (del inglés malicious software), también llamado badware, código maligno, software malicioso, software dañino o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar un ordenador o sistema de información. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

Un software se cataloga como un programa malicioso en función de los efectos que provoque en un computador. El malware no es lo mismo que «software defectuoso»; este último contiene errores peligrosos, pero no de forma intencionada.

Los tipos más conocidos de malware, **virus y gusanos** se distinguen por la manera en que se propagan, más que por otro comportamiento particular.

El término virus informático se usa para designar un programa que, al ejecutarse, se propaga infectando otro software ejecutable dentro de la misma computadora. Los virus realizan a menudo acciones maliciosas, por ejemplo, borrar archivos.

Un gusano es un programa que se transmite a sí mismo, explotando vulnerabilidades en una red de computadoras para infectar otros equipos. El principal objetivo es infectar a la mayor cantidad posible de usuarios, y también puede contener instrucciones dañinas al igual que los virus.

Nótese que un virus necesita de la intervención del usuario para propagarse mientras que un gusano se propaga automáticamente. Teniendo en cuenta esta distinción, las infecciones

transmitidas por correo electrónico o documentos de texto, que dependen de su apertura por parte del destinatario para infectar su sistema, deberían ser clasificadas más como virus que como gusanos.

Otros tipos de malware:

- El término **troyano** suele ser usado para designar a un malware que permite la administración remota de una computadora, de forma oculta y sin el consentimiento de su propietario, por parte de un usuario no autorizado. A grandes rasgos, los troyanos son programas maliciosos que están disfrazados como algo inocuo o atractivo que invitan al usuario a ejecutarlo ocultando un software malicioso. Ese software, puede tener un efecto inmediato y puede llevar muchas consecuencias indeseables, por ejemplo, borrar los archivos del usuario o instalar más programas indeseables o maliciosos.

Los tipos de troyanos son: backdoors, banker, botnets, dialer, dropper, downloaders, keylogger, password stealer.

- El **rogue software** hace creer al usuario que la computadora está infectada por algún tipo de virus u otro tipo de software malicioso, esto induce al usuario a pagar por un software inútil o a instalar un software malicioso que supuestamente elimina las infecciones, pero el usuario no necesita ese software puesto que no está infectado.
- **Ransomware**, también llamados criptovirus o secuestradores, son programas que cifran los archivos importantes para el usuario, haciéndolos inaccesibles, y piden que se pague un «rescate» para poder recibir la contraseña que permite recuperar los archivos. Este tipo de malware está en auge últimamente.
    - Conferencia sobre ransomware
- Las **botnets** son redes de computadoras infectadas, también llamadas “zombis”, que pueden ser controladas a la vez por un individuo y realizan distintas tareas. Este tipo de redes son usadas para el envío masivo de spam o para lanzar ataques DDoS contra organizaciones como forma de extorsión o para impedir su correcto funcionamiento. La ventaja que ofrece a los spammers el uso de ordenadores infectados es el anonimato, que les protege de la persecución policial.
- Las técnicas conocidas como **rootkits** modifican el sistema operativo de una computadora para permitir que el malware permanezca oculto al usuario. Por ejemplo, los rootkits evitan que un proceso malicioso sea visible en la lista de procesos del sistema o que sus ficheros sean visibles en el explorador de archivos. Este tipo de modificaciones consiguen ocultar cualquier indicio de que el ordenador está infectado por un malware. Originalmente, un rootkit era un conjunto de herramientas instaladas por un atacante en un sistema Unix

donde el atacante había obtenido acceso de administrador (acceso root). Actualmente, el término es usado generalmente para referirse a la ocultación de rutinas en un programa malicioso.

4.2. Métodos de protección

Siguiendo algunos sencillos consejos se puede aumentar considerablemente la seguridad, algunos son:

- Tener el sistema operativo y el navegador web actualizados.
- Tener instalado un antivirus y un firewall y configurarlos para que se actualicen automáticamente de forma regular ya que cada día aparecen nuevas amenazas.
- Utilizar una cuenta de usuario con privilegios limitados, la cuenta de administrador solo debe utilizarse cuando sea necesario cambiar la configuración o instLliurexalar un nuevo software.
- Tener precaución al ejecutar software procedente de Internet o de medio extraíble como CD o memorias USB. Es importante asegurarse de que proceden de algún sitio de confianza.
- Una recomendación en tableta, teléfono celular y otros dispositivos móviles es instalar aplicaciones de tiendas muy reconocidas como App Store, Google Play o Tienda Windows, pues esto garantiza que no tendrán malware. Existe además, la posibilidad de instalar un antivirus para este tipo de dispositivos.
- Evitar descargar software de redes P2P, ya que realmente no se sabe su contenido ni su procedencia.
- Utilizar contraseñas de alta seguridad para evitar ataques de diccionario.
- Es muy recomendable hacer copias de respaldo regularmente de los documentos importantes a medios extraíbles como CD, DVD o Disco duro externo, para poderlos recuperar en caso de infección por parte de algún malware, pero solamente si se está 100% seguro que esas copias están limpias.

> “ El método de restauración de los sistemas operativos Windows podría restaurar también archivos infectados que hayan sido eliminados anteriormente por el antivirus, por tanto, es necesario desactivar esta función antes de desinfectar el sistema, y posteriormente reactivarla.

4.2.1 Malware en Lliurex

Lliurex es un sistema GNU/Linux, esto de por sí ya lo hace más seguro que otros sistemas operativos. No se conoce la existencia de ninguna amenaza del denominado software malicioso, malware, en Linux que se haya expandido a un nivel siquiera similar a las amenazas existentes en el sistema operativo Microsoft Windows, por ejemplo. Esto se atribuye en gran parte a que el malware carece usualmente de permisos para realizar actividades nocivas dentro del sistema y a las rápidas actualizaciones frente a vulnerabilidades que se eliminan a diario en GNU/Linux, propias del modelo de software de código abierto. Además, un sistema con GNU/Linux instalado, por lo general, no se parece a otro: Diferentes versiones de núcleo Linux, diferente software instalado, opciones de configuración y características de seguridad estrictas, etcétera. Lo cual dificulta en gran medida la labor de un atacante.

Aun así los virus y ataques malintencionados presentan una amenaza real a los sistemas Linux. Si un binario infectado contiene uno de esos virus al ser ejecutado, el sistema se infectaría. El nivel de infección dependerá de los privilegios del usuario que ejecutó el programa. Si éste fuese una cuenta de superusuario podría llegar a infectar el sistema entero. En caso de un usuario normal, el sistema operativo estaría seguro aunque los datos del usuario no. El virus podría borrar e incluso enviar esos datos a otro equipo remoto. Por otro lado, las vulnerabilidades de escalada de privilegios pueden permitir que malware ejecutándose bajo una cuenta de acceso limitado también se propague por todo el sistema.

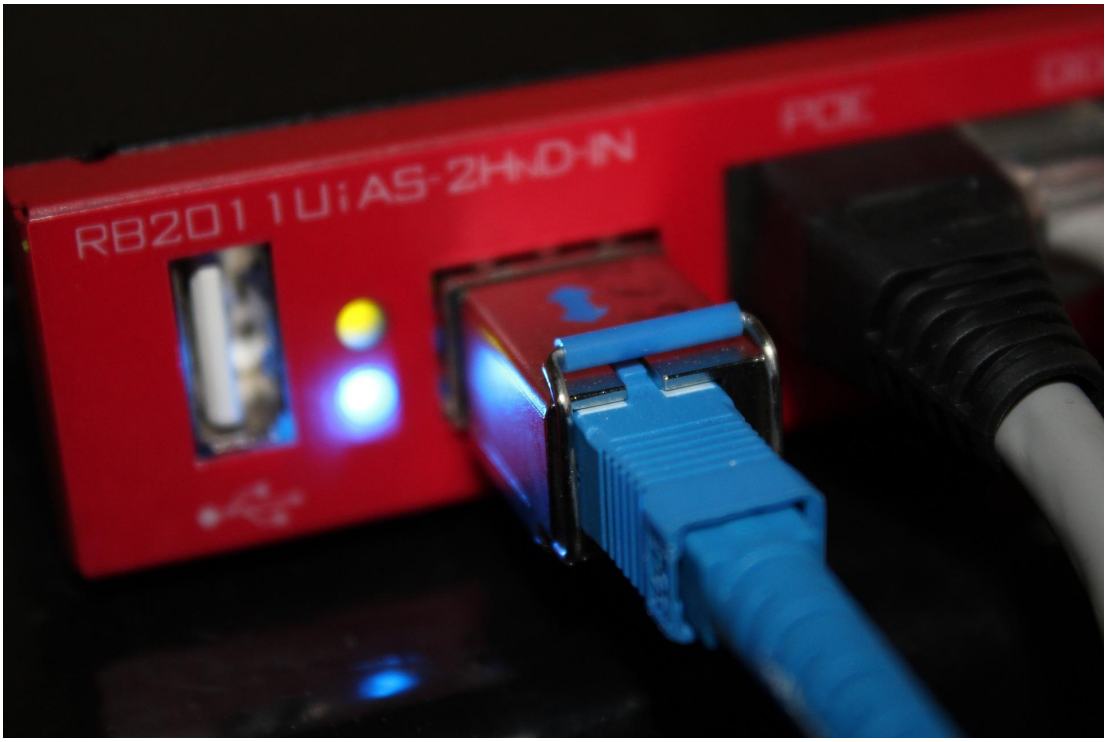
> “El uso de **repositorio de software oficial de Lliurex** reduce las amenazas de instalación de software malicioso, al ser comprobados por los administradores, los cuales intentan asegurar que no se cuele ningún malware en sus repositorios.

4.2.2 Aplicaciones antivirus

Existen varias aplicaciones antivirus multiplataforma disponibles, entre las cuales destacan:

ClamAV (software libre)	BitDefender (propietario)
Antivirus online	ESET (versiones comerciales)
Avast! (versiones gratuita y comercial)	Kaspersky Linux Security (versiones comerciales)
AVG (versiones gratuita y comercial)	Sophos (propietario)

5. Red interna y wifi



Tener unas nociones básicas de esta tecnología es importante para desarrollar adecuadamente nuestra función de coordinadores TIC de centro.

La tecnología WIFI es una opción que nos permite acceder a los recursos de la red local en nuestros dispositivos personales y llevar Internet a todos los rincones del centro. Es necesario tener unas nociones básicas de seguridad. Sin una mínima configuración de seguridad, podemos encontrarnos con problemas como poner en riesgo información importante del centro. Veamos qué podemos hacer para trabajar con una red wifi más segura.

Lo primero es tener claro el uso que le vamos a dar. Hay varios escenarios posibles pero, simplificando, los principales entre los que tendremos que elegir son:

- Uso para tareas de gestión: para que los profesores puedan acceder con seguridad a la aplicación de gestión educativa, manejar datos personales de alumnado, notas de exámenes, etc.
- Uso didáctico: para que profesores y alumnado puedan conectarse a Internet desde las aulas con pizarras digitales, miniportátiles, tabletas, etc. a fin de buscar información, acceder a libros digitales, ver vídeos o cualquier otra actividad.

5.1. Configuración segura

Los routers wifi suelen traer una configuración por defecto sencilla y con un nivel técnico de seguridad razonable. Sin embargo, esta configuración "de fábrica" es muy insegura ya que suelen emplear unos usuarios y contraseñas de administración predeterminados (y conocidos públicamente), y una clave de la wifi que se podría llegar a deducir a partir del nombre de la red o SSID (proveedor de Internet, fabricante y modelo de router).

Por lo tanto, para tener la red wifi protegida es imprescindible realizar algunos cambios en la configuración por defecto del router wifi. Veamos cómo:

- Lo primero es acceder al panel de control del router wifi. Normalmente entrando con el navegador de Internet en la dirección IP del propio router. Nos pedirá introducir el usuario y contraseña de administración (las claves por defecto vendrán en el manual de instrucciones).
- Una vez dentro, deberemos entrar en la opción de menú de ajustes de la wifi: tengamos en cuenta que el nombre de este menú puede ser diferente dependiendo del modelo de dispositivo, por ejemplo "configuración inalámbrica", "wifi", "WLAN", "basic setup", "seguridad", etc. pero los elementos que tenemos que configurar son los mismos. Siempre podemos consultar el manual de instrucciones para asegurarnos:
    - Personalizar el nombre de la red wifi o SSID: procurando que no sea el nombre por defecto, ni sugiera cuál es nuestro proveedor de Internet o fabricante/modelo del router. Además, si nos interesa evitar que accedan los alumnos (para uso de gestión), lo más recomendable es que tenga un nombre "poco llamativo", por ejemplo una palabra formada con las iniciales de una frase o un lema relevante para el profesorado, o un nombre genérico como por ejemplo wireless1606. Valorar la posibilidad de ocultar el nombre de la red, de modo que no aparezca en las pantallas de los dispositivos que estén buscando una wifi. Esto dificulta ligeramente la conexión en un uso diario pero reduce la posibilidad de tener usuarios curiosos intentando entrar. Y viceversa, si queremos darle un uso educativo a la red wifi, lo más sencillo es poner un nombre claro, evidente y visible, por ejemplo IES-AULAS.
    - Configurar un método de cifrado o encriptación robusto: nos aseguraremos de ello eligiendo WPA2 con autenticación de clave compartida (pre shared key) y protocolo AES (también puede aparecer como WPA2-PSK, WPA2-Personal, WPA2-AES). Además tendremos que configurar la "clave de la wifi", es decir la clave que tendremos que poner en los dispositivos clientes para conectarnos a la red wifi. Lógicamente esta clave ha de

ser larga y robusta y no ha de tener relación con el nombre de la red o con nuestra institución educativa.

- Desactivar WPS, también llamado "Wi-Fi Protected Setup" o "WPS Pin": a pesar de que hace que sea más cómodo conectarse a la red wifi, es un método más inseguro (sería algo similar a si tenemos una casa con dos puertas, poner una blindada y la otra normal).

> Hecho esto, acordémonos de guardar los cambios (también puede aparecer como "save", "apply", "siguiente", etc.)

Al guardar los cambios puede que nuestro ordenador nos dé un mensaje de error de conexión y que la página web de configuración del router desaparezca mostrando un mensaje de error... ¡Tranquilidad!, no tenemos por qué haber hecho nada mal. Si nuestro ordenador estaba conectado vía wifi, lo que ha sucedido es que al cambiar el nombre de la red y la clave de la wifi en el router, nuestro ordenador ya no sabe comunicarse con él.

Para continuar tendremos que buscar de nuevo las redes wifi disponibles desde el ordenador para conectarnos al nuevo nombre de red wifi y con la nueva clave. Si habíamos ocultado el nombre de red, tendremos que configurar la red inalámbrica del equipo.

- Vayamos a la opción de menú de ajustes del "sistema", aunque también puede venir indicado con otros nombres como "administración", "configuración", "management", etc.
- Cambiar la clave predeterminada de administración del router: ¡Ojo!, recordemos que esta clave la usaremos solo para acceder al panel de administración del router, no para conectarnos a la red wifi. Deberemos establecer una contraseña robusta y que solo la sepa el coordinador TIC y alguien del equipo directivo. De este modo evitaremos que nadie más pueda acceder al router y "estropear" la configuración.
- Limitar la configuración del router para que solo se pueda modificar desde dentro de la red local ("local management"), pero no desde fuera ("remote management" desde la otra subred o desde Internet). Si nos da la opción, podemos incluso prohibir el acceso a la configuración del router desde los equipos conectados a la red wifi o incluso limitar la configuración a dos equipos concretos (el que solemos utilizar para administración como coordinadores TIC y uno de dirección). Puede parecer más incómodo, pero pensemos que son pocas las ocasiones en que tenemos que acceder al panel de administración del router,

y además es mucho más seguro (siempre que el router se encuentre fuera del alcance de cualquier usuario).

- Finalmente, al guardar los cambios puede que sea necesario reiniciar el router ("save and reboot"), en cuyo caso estará unos segundos sin servicio hasta que vuelva a arrancar.

Al guardar y reiniciar ("save and reboot"," o similar), el router deja de funcionar durante unos segundos (incluso un par de minutos)... Por lo tanto, durante ese tiempo nuestro ordenador perderá la conexión (incluso aunque esté conectado con cable) y el navegador de Internet puede mostrar un mensaje de error... ¿Y qué hacemos?, simplemente esperamos con un poco de paciencia y recargar la página.

5.2. Mantenimiento seguro de la red wifi

Si queremos que nuestra red wifi esté lo más segura posible, conviene que hagamos un pequeño mantenimiento de vez en cuando.

- Cambiar la clave de la wifi periódicamente (al menos cada trimestre), o inmediatamente en cuanto sospechemos que pudiera haber un problema.
- Es relativamente sencillo que algún alumno pueda ver como un profesor introduce una parte de la clave de la wifi (por ejemplo al cambiar de móvil, cuando llega un sustituto, etc.), y a partir de ahí intentar deducir el resto o ir "juntando piezas" para adivinar la clave.
- Apagar el router wifi cuando no se vaya a usar en un cierto periodo de tiempo (por ejemplo durante los periodos de vacaciones). Así evitaremos que nadie "ocioso" tenga la tentación o la posibilidad de intentar saltarse la seguridad del router. Recordemos que la señal wifi traspasa las paredes y puede salir del edificio.
- Comprobar de vez en cuando, o cuando tengamos alguna sospecha, que no haya ningún dispositivo conectado indebidamente a la red wifi. Lo podemos hacer entrando al panel de administración del router y revisando el apartado de información del "sistema", "estado", "conexiones", "logs" o similar.
- Asegurarnos de que nuestro router wifi no cae en manos de ninguna botnet o red zombi (sí, también los routers se pueden infectar y convertirse en zombis). Para ello lo más sencillo es configurar el router wifi de manera segura y utilizar el servicio antiBotnet de OSI, por ejemplo descargando el plugin para el navegador de tu ordenador o instalando la aplicación CONAN mobile de INCIBE en tu dispositivo móvil.

5.3. Buen uso de la red

Ahora bien, para que todo esto funcione necesitamos que nuestros compañeros, y en su caso alumnos, utilicen la red wifi adecuadamente. Aunque parece algo evidente y de sentido común, necesitamos hacer una pequeña labor de sensibilización y pedagogía con ellos, algunos puntos en los que podemos hacer incapié:

- **Usar la red wifi para su propósito**. El acceso a contenidos de ocio, especialmente los vídeos, u otros que se salen del ámbito educativo, puede sobrecargar la red y reducir la velocidad de la misma además de aumentar innecesariamente los riesgos de infección.
- Por otra parte, si hemos dicho que la red wifi se va a utilizar solo para gestión, no debemos emplearla con nuestro alumnado. De la misma manera, si la vamos a utilizar solo didácticamente, no debemos emplearla para acceder ni a la aplicación de gestión educativa, ni a documentación profesional o privada.
- **La clave de la wifi también es privada**, máxime si utilizamos la red wifi para gestión. No se debe compartir con nadie, ni llevarla apuntada en un papel o cuaderno (ya que puede ser leída por otra persona).
- También debemos tener mucho cuidado de no introducirla en nuestros dispositivos delante de nadie, pues podrían hacerse con ella.
- **Proteger los dispositivos que se vayan a conectar a la red wifi**, asegurándose de que tengan instalado y actualizado un **antivirus**, cuidando las aplicaciones que se instalan (de confianza y solo desde las tiendas oficiales), haciendo un uso responsable y con sentido común.

5.4. Freeradius

Cada vez son más los programas que permiten averiguar, en unos pocos minutos, la clave de red y aún más fácil cuando son instalados en dispositivos móviles.

Esto nos lleva a plantearnos nuevos retos que permitan hacer más segura nuestra red, una manera muy eficiente es utilitzar RADIUS, un protocolo ampliamente empleado para controlar el acceso a servicios en red. En particular FreeRADIUS, viene preconfigurada en el servidor Lliurex haciendo muy sencilla la configuración en nuestro centro para el acceso a una red inalámbrica.

RADIUS (Remote Authentication Dial-In User Server) es un protocolo que nos permite gestionar la “autenticación, autorización y registro” de usuarios remotos sobre un determinado recurso. La tupla “autenticación, autorización y registro” es más conocida como AAA, al ser este su acrónimo de su

denominación original inglesa “Authentication, Authorization, and Accounting”. Veamos a continuación a qué se refiere cada uno de estos términos:

- **Autenticación** (authentication): Hace referencia al proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. El proceso de autenticación se realiza mediante la presentación de una identidad y unas credenciales por parte del usuario que demanda acceso. Un tipo habitual de credencial es el uso de una contraseña (o password) que junto al nombre de usuario nos permite acceder a determinados recursos. Otros tipos más avanzados de credenciales son los certificados digitales.
- **Autorización** (authorization): Se refiere a conceder servicios específicos (entre los que se incluye la “negación de servicio”) a un determinado usuario, basándose para ellos en su propia autenticación, los servicios que está solicitando, y el estado actual del sistema. Es posible configurar restricciones a la autorización de determinados servicios en función de aspectos como, por ejemplo, la hora del día, la localización del usuario, o incluso la posibilidad o imposibilidad de realizar múltiples “logins” de un mismo usuario.
- **Registro** (accounting a menudo traducido también como contabilidad): Se refiere a realizar un registro del consumo de recursos que realizan los usuarios. El registro suele incluir aspectos como la identidad del usuario, la naturaleza del servicio prestado, y cuándo empezó y terminó el uso de dicho servicio.

Un uso de RADIUS que queremos enfatizar, es la autenticación en redes inalámbricas (Wi-Fi), sustituyendo métodos más simples de clave compartida (pre-shared key, PSK), que son bastante limitados al gestionar una red cuando esta alcanza un determinado tamaño.

> “ Enlaces de ampliación Freeradius:
>
> - Inicializar Freeradius en Lliurex
> - Freeradius filtrado de acceso por grupos en Lliurex
> - Configurar Freeradius en Windows Server

Si deseas ampliar información sobre Ciberseguridad en las Comunicaciones Inalámbricas en entornos profesionales sigue este enlace.

Sugerencia:

Suscríbete al boletín quincenal del Centre de Seguretat TIC de la Comunitat Valenciana para estar al día de las principales noticias y alertas, del mundo de la seguridad.

6. Bibliografía

- Wiki de Lliurex. https://wiki.edu.gva.es/lliurex/
- SAI. http://sai.edu.gva.es
- Internet Segura For Kids. https://www.is4k.es/
- Seguridad física. http://www.rediris.es/cert/doc/unixsec/node7.html
- Gestión de contraseñas en Lliurex. http://wiki.edu.gva.es/lliurex/tiki-index.php?page=Gestión+de+contraseñas
- Malware. https://es.wikipedia.org/wiki/Malware
- Canal de seguridad informática en Telegram. https://t.me/seguridadinformatic4
- Cortafuegos https://es.wikipedia.org/wiki/Cortafuegos_(informática)
- Recopilación de enlaces sobre seguridad. https://www.diigo.com/user/sasogu?query=seguridad
- Normativa de la D.G. de Tecnologies de la Informació de la CEICE. http://www.ceice.gva.es/es/web/innovacion-tecnologica/normativa
- Normativa e Instrucciones de Infraestructura Educativa de la CEICE. http://www.ceice.gva.es/es/web/contratacion-educacion/normativa-e-instrucciones

7. Autoría

Elaborado por:

Equipo de Coordinación TIC de la Unidad de Soporte al Servicio de Informática para los Centros Educativos
Dirección General de Tecnologías de la Información y las Comunicaciones
Conselleria de Hacienda y Modelo Económico

Y actualizado por:

Equipo de Coordinación TIC del Servicio de Planificación y Gestión de la Formación Permanente del Profesorado
Subdirección General de Formación del Profesorado
Secretaría Autonómica de Educación e Investigación
Conselleria de Educación, Cultura y Deporte.

Obra publicada con Licencia Creative Commons Reconocimiento Compartir igual 4.0

Actividades

Elige una de las dos siguientes:

1. **Actividad tarea.**
   Comprueba si tu usuario y contraseña en Internet han sido hackeados en alguna ocasión, introduce tu dirección de correo habitual en la siguiente dirección web **https://haveibeenpwned.com/ y envía una captura de pantalla**.
   Puedes encontrar de dónde salen los datos en esta otra web: https://hacked-emails.com/

   ¿Qué hacer si te hackearon?
   • Cambia inmediatamente tu contraseña, siguiendo los criterios aprendidos en el tema.
   • Utiliza un gestor de contraseñas, por ejemplo, LastPass o https://1password.com/
   • Habilita un código o llave de seguridad adicional a tu contraseña
   • Usa la verificación en dos pasos si el servicio ofrece esta posibilidad (protege tu cuenta también con tu teléfono móvil).

2. **Actividad tarea.**
   Comprueba que la red de ordenadores que utilizas habitualmente está libre de botnets a través del **Servicio online antibotnet de la OSI y envía una captura de pantalla** con el resultado de hacer el chequeo de tu conexión.

   Te recomendamos la instalación de este plugin para Chrome o Firefox, para un chequeo continuo y que estés al día de los consejos para prevenir infecciones y utilizar herramientas de seguridad en tus dispositivos.