Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.
CONSEJERÍA DE ECONOMÍA, INNOVACIÓN, CIENCIA Y EMPLEO

AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe de divulgación

Recomendaciones de seguridad en redes de acceso público

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-4348-130924*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*24/09/2013*
N° de Páginas	*1 de 20*

1 TABLA DE CONTENIDOS

2 OBJETO

El objeto de este documento es proporcionar recomendaciones de seguridad aplicables en despliegues de redes orientadas al uso de personal ajeno a la organización, y por tanto, fuera del alcance de las políticas de seguridad y conducta aplicadas al personal que trabaja para la organización.

Se enumerarán y describirán las características de este tipo de escenarios, así como los riesgos más comunes que nos vamos a encontrar en ellos. En base a éstos, se proporcionará una propuesta de posibles controles de seguridad destinados a reducir y mitigar los problemas de seguridad ligados a este tipo de despliegues, así como reducir el riesgo.

3 ALCANCE

Este documento va destinado al personal técnico de la Junta de Andalucía y al público en general. En él se estudian problemas de seguridad en redes interconectadas a la red de la organización y destinadas al uso de personal externo a la organización. Se proponen recomendaciones y controles para la mejora de la seguridad en estos escenarios.

4 INTRODUCCIÓN

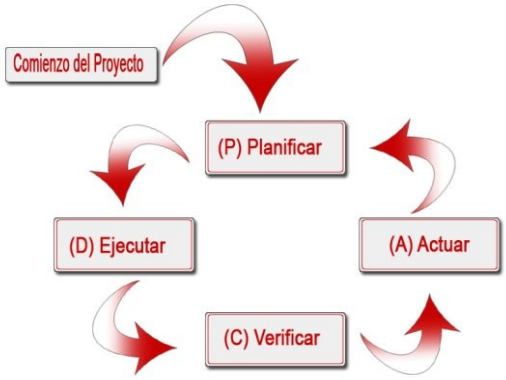
El paso a la administración electrónica y el auge de la sociedad de la información ha creado en un gran número de organismos públicos la necesidad de poner a disposición de las personas medios que les permitan acceder a los diferentes servicios que se ofrecen.

Con ello entran en juego en nuestra organización un tipo de redes dedicadas al uso de usuarios externos a la organización, aunque interconectadas a la red corporativa. Estas redes suelen permitir el acceso a Internet y/o a algunos servicios internos de la red corporativa.

No obstante, pese a estar conectadas con las redes internas de la organización, deben ser consideradas de forma diferente. Sus usuarios, en general, serán ajenos a la política de la organización y no estarán vinculados a contratos de confidencialidad, de conducta, buenas prácticas, etc. Esto genera un claro problema de seguridad si no es tenido en cuenta a la hora de llevar a cabo su despliegue.

El objetivo de este documento es proporcionar una serie de recomendaciones a aquellas organizaciones que cuenten con **redes de acceso público** y les permita identificar las características que pueden impactar directamente sobre la seguridad (o inseguridad) de su organización. En base a estas peculiaridades se proporcionarán algunas medidas o controles adecuados a aplicar en este tipo de contextos.

5 Estrategia de seguridad en redes de acceso público



La mejor forma de llevar a cabo un plan de seguridad en cualquier tipo de escenario es comenzar definiendo una estrategia previa de actuación que nos permita analizar el entorno, sus particularidades, los problemas y riesgos más importantes que hay que mitigar, posibles soluciones a éstos y métodos para comprobar de forma continua que todo funciona correctamente o si podría mejorarse.

- **Planificar**: En esta fase realizaremos lo siguiente:
  - Un análisis de riesgos que ofrezca una visión global del escenario sobre el que vamos a trabajar.
    - Se deberán identificar todas las características de éste, así como los activos y actores que participarán.
    - Identificación de amenazas.
    - Obtención del riesgo.
  - Adaptación de la política de seguridad corporativa a este tipo de entornos, o definición de una dedicada a estos casos.
  - Identificación y definición de controles para minimizar los riesgos identificados.

- **Ejecutar**:
  - Implementación de los controles de seguridad escogidos en la fase anterior. En esta fase se llevará a cabo el despliegue de elementos TIC (software, hardware, ...), pero también se creará o revisará la documentación necesaria (políticas, procedimientos, instrucciones y registros).
  - Concienciación y formación del personal, tanto interno como externo, de cara a que se conozcan los controles implantados, y sobre todo la política de seguridad que debe ser aplicada.

- **Verificar**: En este punto se procederá a evaluar la eficacia y éxito de los controles implantados. Es por esto que toman especial importancia los registros (evidencias) que dejan los diferentes controles.

- **Actuar**: En esta fase se llevarán a cabo las labores de mantenimiento del sistema así como labores de mejora y corrección si, tras la verificación, se ha detectado algún punto débil. Esta fase se suele llevar en paralelo con la verificación, de tal forma que al detectarse una deficiencia se actúa directamente sin esperar a tener la fase de verificación completada para comenzar con las tareas de mejora y corrección.

5.1 Análisis de riesgos en redes de acceso público

Hay que partir de la premisa de que este tipo de redes deben ser consideradas como inseguras por defecto, y por tanto, de cara a su interacción con las redes internas, deberán ser tratadas como cualquier otra red insegura, con la salvedad de que su responsabilidad es de nuestra competencia.

Es muy posible que la gran mayoría de los usuarios de una red de acceso público no se encuentren formados en buenas prácticas de seguridad sobre el manejo seguro de las TIC. Un gran número de riesgos con los que tendremos que lidiar serán consecuencia directa del mal uso que realicen los usuarios de los servicios TIC ofrecidos.

En función a las características específicas de entorno desplegado, descubriremos que nuestra red está expuesta a una serie de riesgos que deberán ser identificados y analizados.

Mediante un análisis de riesgos identificaremos los activos TIC desplegados en la red o accesibles desde la misma, sus vulnerabilidades y amenazas a las que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas. Esto nos permitirá determinar los controles de seguridad más adecuados que tendremos que implementar para evitar o disminuir la ocurrencia del riesgo.

5.1.1 Análisis del escenario

El primer punto sobre el que tendremos que invertir esfuerzos es identificar todas aquellas características que nuestra red de acceso público tiene y los requisitos que se deben cumplir.

5.1.1.1 Requisitos

La seguridad implementada en una red de acceso público debe poder llevarse a cabo sin llegar a sacrificar ninguno de estos requisitos.

- **Acceso a cualquier persona**. Este tipo de redes están orientadas a cualquier usuario, de cualquier condición o perfil. Cualquier persona podrá hacer uso de los servicios ofrecidos por una red de acceso público. En general con esto nos referimos a personas que no son de la organización.

- **Disponibilidad de los servicios**. Se debe garantizar que los servicios ofrecidos están siempre disponibles a los usuarios.

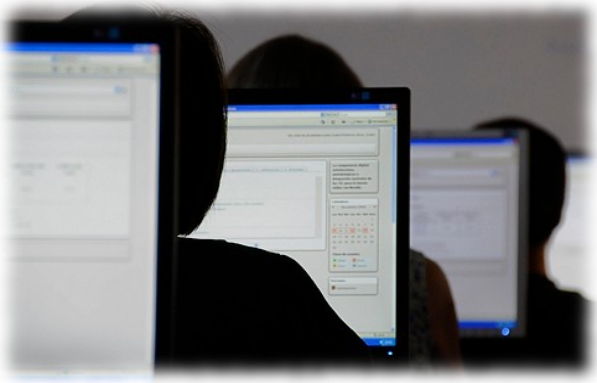
- **Privacidad de los usuarios**. Se debe garantizar la privacidad de los datos que los usuarios manejan mientras hacen uso de los servicios ofrecidos por una red de acceso público, incluso los de aquellos que sean más despistados (documentos e información copiada en local, datos guardados en navegadores, histórico de sitios visitados, comunicaciones, etc).

- **Cumplimiento legal**. Puesto que este tipo de redes están orientadas a que personas externas a la organización las use, hay que considerar todos aquellos aspectos legales que pudieran convertirse en un problema si no los tenemos en cuenta. Algunos temas como filtros de seguridad para el acceso de menores, licencias (software, libros, etc), accesibilidad, velar para que nuestra red no sea usada en acciones ilegales (subida de material pirata, acoso, etc).

5.1.1.2 Servicios

Identificar claramente los servicios que se desean proporcionar. No todas las redes de acceso público proporcionan los mismos servicios. Algunos de los más comunes suelen ser:

- Navegación web a través de Internet.
- Acceso a correo electrónico.
- Accesos a ciertos servicios de la Intranet (P.ej: catálogo de una biblioteca, aulas virtuales, etc.).
- Conexión inalámbrica para acceso a Internet de equipos de usuarios.
- Préstamo de equipamiento TIC.
- Servicio de impresión de documentos.
- Acceso a aplicaciones de escritorio.
- Servicio de videoconferencia.
- Etc.



5.1.1.3 Activos

Debemos de identificar los activos que se han desplegado para poder proporcionar el servicio que deseamos. Entre estos tendremos:

- Puestos con ordenadores.
- Ordenadores portátiles para préstamo.
- Software de escritorio (P.ej: herramientas ofimáticas).
- Documentos.
- Impresoras.
- Webcam
- Etc.

5.1.2 Identificación de amenazas

El siguiente paso, una vez identificado lo que tenemos, es saber a qué amenazas están expuestos nuestros activos, servicios, usuarios, así como toda la organización. A continuación se listan una serie de amenazas muy comunes en redes de acceso público.

- **Deficiencias de seguridad derivadas de los perfiles de usuarios**: Si los usuarios y los permisos asociados de los usuarios no están correctamente definidos y configurados existe el riesgo de que éste tenga capacidad de realizar acciones que puedan llegar a dañar o a degradar el funcionamiento del sistema (instalación de programas, cambios en configuraciones, borrado de datos, etc).

  Además de los fallos derivados de la definición de los perfiles de usuarios, pueden existir fallos en las políticas de seguridad asociadas a un determinado tipo de usuarios. Si no se configuran adecuadamente estas políticas, donde se define a lo que está o no autorizado a hacer el usuario, cabe la posibilidad de que un usuario tenga acceso a partes restringidas de la Intranet como redes de ofimática, redes de servidores, etc.

- **Explotación de fallos de seguridad y malas configuraciones**: Se trata de la posibilidad que tiene el usuario de aprovecharse de algún fallo de seguridad existente en algún programa instalado o en el propio sistema. Existen muchos fallos de seguridad derivados de malas configuraciones, pero por norma general, el principal motivo de la presencia de fallos de seguridad en un sistema es debido a no actualizar el entorno TIC o no contar con una política de actualización adecuada.

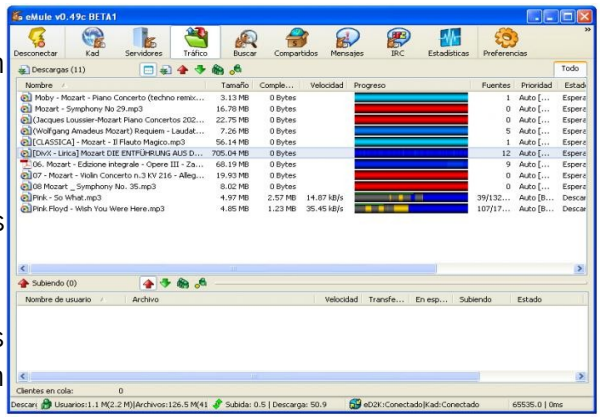
- **Denegación de servicios**: De manera accidental o intencionada existe el riesgo de que se produzcan la denegación de alguno de los servicios ofrecidos en la red pública o incluso relacionados con la red interna de la organización.

- **Infección por malware**: Un usuario, a través de múltiples vías, podrá llegar a infectar y comprometer los equipos conectados a la red. Algunas vías de infección son:
  - Acceso a sitios web dañinos y de baja reputación.
  - Descarga de programas maliciosos de la web, correo electrónico u otros.
  - Conexión de dispositivos infectados en equipamiento corporativo.
  - Conexión a la red de equipos infectados y propagación de malware (gusanos).

- **Propagación de amenazas**: No establecer controles adecuados para contener las amenazas entorno a la red de acceso público puede provocar que éstas se extiendan por todos los equipos conectados a la red, incluso que se propague por redes internas de la organización. Habría que tener en cuenta los siguientes vectores de propagación:

- **Propagación de amenazas a la Intranet**: Si la red de acceso público no se encuentra correctamente configurada o no está separada de la del uso interno de la organización, es posible que se produzcan accesos no autorizados o ataques a redes y servicios de uso interno en la organización.
- **Propagación de amenazas en la red local**: Un usuario malintencionado o un equipo infectado que se conecte a la red puede intentar comprometer a otros usuarios y equipos conectados dentro de la misma red local (escucha de tráfico y captura de contraseñas, servicios falsos, ataques, propagación de infecciones, etc).
- **Propagación de amenazas hacia Internet**: Las redes de acceso público suelen ser un blanco de los atacantes para ser usadas como origen de ataques a terceros de una manera anónima (escaneos, ataques de denegación de servicio, suplantación de identidad, etc.). Este tipo de acciones pueden ser realizadas de forma intencionada por algún usuario, o de forma inconsciente, por ejemplo, por acción de algún software malicioso instalado en el equipo.

- **Realización de acciones ilegales**
  - Publicación y descarga de contenido con copyright.
  - Uso de software pirata.
  - Cyberacoso.
  - Envío de correos fraudulentos (spam/phishing).



  Este tipo de acciones pueden tener efectos negativos en nuestra organización e incluso en nuestra reputación.

- **Daños físicos:**
  - **Daños al equipamiento**: En el caso de que el organismo proporcione el equipamiento existe la posibilidad de que se produzcan daños al material proporcionado por deterioro, mal uso o vandalismo.
  - **Robo de equipamiento TIC.**

- **Violación de políticas de conducta**: Además de las amenazas anteriormente citadas, se deben contemplar todas aquellas acciones no permitidas por las políticas de la organización.

5.1.3 Cálculo del riesgo

El último punto del análisis de riesgo es el cálculo del riesgo asociado a cada amenaza identificada y para cada activo de la red. Habrá que tener en cuenta su probabilidad de ocurrencia frente al impacto en la organización que provocaría si se llegara a manifestar.

5.2 Definición de la política de seguridad y conducta

Tras identificar qué riesgos pueden afectar a nuestra red según el tipo de despliegue que hayamos definido, deberemos estipular el conjunto de normas y procedimientos que regularán el uso de la información y de los sistemas desplegados en nuestra red de acceso público.

Posiblemente ya contemos con un documento donde se definan las políticas marcadas por la organización por lo que tendremos que estudiar qué puntos pueden ser aplicables, cuales no, y cuales necesitarían ser adaptados.

En el siguiente enlace podemos ver un ejemplo de política de seguridad. En este caso, la de la biblioteca pública de San Francisco: http://sfpl.org/index.php?pg=2000004302

5.3 Definición de controles

Una vez que comprendemos nuestro entorno especifico, hemos identificado los riesgos de seguridad a los que está expuesto y tenemos definida una política de seguridad debemos estudiar qué controles de seguridad son los más adecuados. En el punto 6 de este documento presentaremos los controles más usuales que se aplican en este tipo de escenarios.

5.4 Implementación de controles

Una vez definidos los controles de seguridad el siguiente paso es implantarlos en nuestra red.

5.5 Concienciación

Este tipo de normas y controles deberán ser conocidos por los usuarios para que se lleven a cabo. Por ello se deberán establecer mecanismos para hacer llegar esta información, ya sea con folletos, carteles, u otros medios.

5.6 Revisión

En la fase de revisión debemos comprobar que las medidas o controles aplicados funcionan correctamente, corrigen los fallos de seguridad a los que están destinados y lo hacen de una forma eficiente y apropiada al medio. Para ello, es necesario, pasado un tiempo previamente definido, estudiar los resultados actuales y compararlos con los resultados esperados.

Finalmente, si se han detectado que los resultados no son los esperados, alguna deficiencia o algo que podría mejorarse, será necesario tenerlo en cuenta en la siguiente fase.

5.7 Realimentación

La estrategia propuesta es cíclica y debe ser mejorada continuamente.

Las organizaciones cambian constantemente, la tecnología evoluciona y las amenazas también. El proceso de proteger la información no puede ser concebido como algo que tiene principio y fin. Se requiere de una trabajo activo y continuo para obtener resultados.

6 CONTROLES DE SEGURIDAD

A continuación se proporciona una lista de controles orientados a evitar o al menos reducir gran parte de los riesgos que pueden derivarse de las amenazas anteriormente citadas.

El listado de controles se ha clasificado en 3 tipos:

- Controles físicos: Relativos a seguridad física en general.
- Controles de sistema: Se apoyan en herramientas software o hardware.
- Controles de red: Relativos a servicios en red.

Como ya se ha venido diciendo, cada escenario concreto requerirá o no la implementación de éstos u otros controles no contemplados en esta lista. Incluso podrán existir casos en los que, en base a los resultados obtenidos en el análisis de riesgo, se determine no implementar algún control.

6.1 Controles físicos

- **Control de acceso:** Tener un registro de todos los accesos que se han tenido lugar en nuestra red es esencial de cara a identificar futuros problemas. Por ello es conveniente contar con algún sistema que nos permita tener un registro de usuarios y accesos a los servicios ofrecidos. En estos sistemas se mantendrán registro de fecha, hora, usuario, inicio, fin, equipo usado y cualquier otro parámetro que nos ayude, en caso de incidente, a determinar qué usuario o máquina ha hecho esta o aquella acción en un momento determinado.

- **Conexión de dispositivos externos**: En general, siguiendo el principio de mínimos privilegios, se debería prohibir la conexión de todo tipo de dispositivo externo en un equipo corporativo localizado en una red de acceso público. Este tipo de dispositivos suponen un foco muy importante de propagación de malwares, copiado de software pirata, fuga de datos, etc.

  Puede considerarse que la restricción de conectar dispositivos externos es excesiva. En ese caso, como mínimo se deberían configurar los sistemas para **evitar el auto-arranque de este tipo de dispositivos**. Existen un gran número de malwares que al infectar un dispositivo de este tipo, modifican la configuración de auto-arranque para ser ejecutados de forma automática en cuanto son conectados. Esta medida, en caso de permitir la conexión de dispositivos externos, evitará que, en caso de que un dispositivo externo (pendrive USB, DVD, disco duro externo, etc.) esté infectado por un malware de este tipo, se ejecute de forma automática.

- **Protección del equipamiento:** En caso de que el acceso a red se realice usando equipamiento corporativo, éste deberá estar protegido ante un mal uso o robo. Hoy en día muchos de los sistemas de computación vienen preparados para que puedan ser protegidos de forma física por medio de cadenas u otros. También pude ser una buena idea asegurar el equipamiento o hacer uso de los sistemas de alquiler de PCs previniendo que el uso por distintos usuarios los desgaste o dañe.

- **Inventariado:** Es muy necesario mantener un inventario que nos permita conocer en todo momento qué material hay a disposición de los usuarios, cuales están en uso, cuales libres, cuales se han "prestado" y por cuanto tiempo, etc.

6.2 Controles de sistema

En este punto se tratarán una serie de controles que se apoyan en el uso de herramientas software o hardware.

- **Protección de la BIOS:** Denegar el acceso de los usuarios a las opciones de la BIOS de cualquier equipo.

- **Plataformado homogéneo:** De cara a facilitar las labores de administración de los equipos conectados a la red, un plataformado homogéneo será muy recomendable.

- **Uso de cuentas de usuarios:** Para mantener un mayor control sobre los accesos a los servicios ofrecidos es más que recomendable obligar a que su uso sea a través de cuentas de usuario previamente registradas. Esto es aplicable tanto a los accesos a través de equipos propios de la organización como a los accesos con equipos propios de los usuarios, usando por ejemplo, la red WiFi.

- **Administración de privilegios de usuarios:** Éstos deberán tener los **privilegios mínimos** que les permitan actuar con los servicios ofrecidos. Para mayor facilidad en la gestión de perfiles de usuarios es recomendable usar grupos a los que se les configuren políticas aplicables a todos los usuarios incluidos en el grupo.

- **Mantenimiento del software actualizado**: Es fundamental contar con una política de actualización periódica de los elementos que componen la infraestructura TIC desplegada. Las actualizaciones de los programas vienen justificadas principalmente por dos motivos:
  - Corregir las vulnerabilidades conocidas.
  - Proporcionar nuevas funcionalidades o mejoras respecto a las versiones anteriores.

- **Configuración de auto arranque:** Como parte de la lucha anti-malware y otras posibles acciones maliciosas, será conveniente deshabilitar la función de auto arranque de dispositivos extraíbles.

- **Limite de recursos:** Como parte de la misma configuración de usuario, sería imprescindible limitar los recursos del sistema (disco duro, red, otros) de tal modo que un usuario o programa usado por un usuario, no pueda llegar a realizar una denegación de servicio de forma intencionada o por error.

- **Uso de antivirus:** Hoy en día es casi impensable usar cualquier plataforma sin el uso de un antivirus **actualizado** y de confianza. Es más, se recomienda el uso de distintos sistemas de detección de amenazas (antispyware, antirootkits, ...) ya que no todos detectan con igual eficacia ni se actualizan con la misma frecuencia.

- **Limpieza de sesiones de usuarios** para garantizar la privacidad de los datos.

- **Política de restauración de sistemas:** Una práctica habitual es la restauración automatizada de los sistemas de forma periódica. Este método nos permite mantener en perfecto estado cada día nuestras máquinas a pesar de la posible degradación de éstas por su uso.

- **Securización de los navegadores:** Por regla general, el servicio más usado en una red de acceso público será la navegación web. Por este motivo, los navegadores web se convierten en una herramienta a la que le debemos prestar atención y debemos de securizar. Entre las medidas que debemos contemplar están:
  - Mantenimiento de versiones actualizadas.
  - Controlar o denegar la instalación de extensiones y/o complementos.
  - Control de descargas.

- **Límites de tiempo de uso:** Con el fin de que los servicios estén disponibles para todos los usuarios se puede establecer límites de tiempo programados para hacer un uso continuado de los equipos. Este límite deberá ser adaptado a cada situación concreta.

  Esto además de garantizar la disponibilidad del servicio a todos los usuarios, podría limitar la posibilidad de que un usuario realice un ataque continuado desde la red.

6.3 Controles de red

La función principal de una red pública es precisamente el acceso a la "RED" pudiéndose dividir ésta en Intranet e Internet. Casi todos los puntos de securización hasta este momento han servido de una forma más o menos directa para conseguir la seguridad en red. No obstante, en este punto nos centraremos en algunos controles de seguridad orientados a la protección de las conexiones habilitadas en una red de acceso público, y de las redes que interconecta.

- **Segregación de redes:** La conexión de una red de invitados o pública a nuestro entorno, por definición ya supone un riesgo para el resto de redes de la organización. Para mantener aisladas estas redes de nuestra redes internas tendremos que segregarlas de las mismas. Para ello será muy conveniente el uso de VLANs, de tal modo que se pueda delimitar el encaminamiento y aplicar políticas especificas.

- **Políticas de navegación:** Se deberán definir políticas de navegación para los usuarios. Estas políticas no tienen por que ser aplicadas por el usuario sino mediante cortafuegos, proxys, IPS y otros.
  - Control de descargas: En este punto, debemos de establecer fuertes controles sobre la descarga de software desde Internet. En general, en este tipo de escenarios, todo lo que se descargue de Internet deberá ser considerado como inseguro.
  - Filtrado de contenidos: Controlar el acceso a páginas de contenido explícito y/o peligrosas.

- **Restricción de recursos de red:** Para evitar que un usuario sature la red y no limite los servicios de otros usuarios conectados a la misma se podrán usar sistemas de regulación de tráfico en base a tecnologías QoS.

- **Herramientas de seguridad perimetral**: El uso de firewalls, proxys, IDS's, antivirus de red..., nos permitirá identificar y proteger de muchos ataques externos, conocer si algún equipo interno está realizando acciones extrañas, controlar el acceso entre subredes, etc.

- **Portales cautivos**: Se trata de programas que vigilan el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal. Estos portales son una buena solución de seguridad para este tipo de escenarios, permitiendo restricciones de QoS, políticas de navegación, etc.

7 ESCENARIOS DE EJEMPLO

A continuación vamos a plantear 3 casos muy habituales de redes de acceso público. Sobre estos escenarios se plantearán los riesgos más usuales que nos vamos a encontrar y posibles controles a aplicar para su mitigación.

- **Nota**: C = Control

7.1 Red de acceso a usuarios de una biblioteca

Como primer escenario planteamos una red de una biblioteca. En ésta se ofrece a cualquier persona la posibilidad de usar equipos informáticos propios de la biblioteca. Desde éstos es posible acceder a Internet y a determinados servicios corporativos relacionados con la biblioteca (catálogo de libros, servicio on-line de préstamo, etc.).

Servicios ofrecidos:

- Uso de ordenadores corporativos.
- Acceso a Internet.
- Acceso a servicios limitados de la Intranet.

Riesgos y controles

- **Uso de ordenadores corporativos.**
  - Ejecución de programas que no se permiten.
    - C: Limitación de permisos de usuarios.
  - Acceso a archivos del sistema.
    - C: Limitación de permisos de usuario.
  - Instalación de software pirata.
    - C: Limitación de permisos de usuario.
  - Instalación de malware.
    - C: Limitación de permisos de usuario.
    - C: Uso de antivirus actualizado.
  - Alteración de configuraciones hardware y de arranque.
    - C: Protección de la BIOS con contraseña.
  - Conexión de dispositivos externos
    - Si está infectado puede infectar al equipo y propagarse por la red.
    - Se puede copiar software ilegal en el equipo que traiga en el dispositivo.
      - C: Denegar conexiones de dispositivos de almacenamiento externo.
      - C: Deshabilitar función de auto-arranque.
  - Realización de acciones ilícitas anónimas.
    - C: Uso de usuarios registrados.

        - C: Concienciar a los usuarios y darles a conocer las normas recogidas en la política de conducta.
    - Degradación del sistema:
        - C: Restauración periódica de los sistemas.

- **Acceso a Internet**
    - Descarga e instalación de código malicioso.
        - C: Bloquear la posibilidad de descarga de software de Internet.
    - Acceso a sitios maliciosos, de baja reputación, de contenido explícito y/o violento, etc.
        - C: Filtrado de contenidos.
        - C: Concienciar a los usuario y darles a conocer las normas recogidas en la política de conducta.
    - Ataques internos entre los equipos de la red local.
        - C: Configuraciones de red que eviten la comunicación directa entre equipos conectados a la misma red.
    - Conexión de equipos de usuarios a la red.
        - Equipos infectados
            - C: Acceso al servicio a través de portal cautivo.
            - C: Antivirus de red
        - Equipos con software no identificado.
            - C: Concienciar a los usuario y darles a conocer las normas recogidas en la política de conducta.
    - Realización de ataques anónimos.
        - C: Limitación de privilegios.
        - C: Limitación de recursos (ancho de banda, tiempo...).
        - C: Monitorización de la red.
    - Realización de acciones ilegales (cyberacoso, publicación de contenido con copyright, ...).
        - C: Aplicación de la política de filtrado de contenidos corporativa.
        - C: Concienciar a los usuario y darles a conocer las normas recogidas en la política de conducta.
        - C: Monitorización de la red.

- **Acceso a servicios limitados de Intranet**
    - Acceso a servicios internos y redes no autorizadas.
        - C: Segregación de redes.
        - C: Control perimetral.
        - C: Monitorización de red.

7.2 Kiosko interactivo

En este escenario tenemos un kiosko interactivo situado en un lugar público y accesible a cualquier persona. El kiosko está dotado de una pantalla táctil y la aplicación ejecutada es un navegador web (Internet Explorer) en modo kiosko.

Cuando el equipo arranca, de forma automática se realiza un login y se ejecuta el navegador en modo kiosko. La página por defecto proporciona al usuario un menú con accesos a las áreas de servicios ofrecidos.

Servicios ofrecidos:

- Acceso vía web a servicios de la Intranet.

Riesgos y controles:

- Realización de acciones privilegiadas en el sistema.
  - C: Perfil de usuario por defecto:
    - Usuario por defecto para el uso del sistema (el mismo para cualquier usuario).
    - Auto-login de usuario por defecto al arrancar el sistema.
    - Políticas muy restrictivas. Éstas deberán, al menos, denegar lo siguiente:
      - Acceso al escritorio.
      - Acceso a recursos locales (disco duro, dvds, etc).
      - Guardado de datos.
      - Instalación de aplicaciones.
      - Realización de cambios en la configuración de aplicaciones o del sistema.
      - Acceso a terminal de comandos directamente o a través de otras aplicaciones que el usuario si puede ejecutar (por ejemplo, a través de web).
      - Reiniciar o apagar el sistema.
      - Cerrar la sesión del usuario por defecto.
      - Cerrar la aplicación de kiosko.

- Infección por malware.
  - C: Denegar conexiones de dispositivos externos.
  - C: Uso de antivirus actualizado.
  - C: Monitorización de conexiones.

- Explotación de brechas de seguridad en el (navegador web).
  - C: Actualización y aplicación de los últimos parches de seguridad al navegador web y al sistema operativo.

- Acceso a servicios internos y redes no autorizadas.
  - C: Segregación de redes.

- C: Control perimetral.
- C: Monitorización de red.
    - Conexión de equipos de usuarios a la red.
        - Equipos infectados
            - C: Acceso al servicio a través de portal cautivo.
            - C: Antivirus de red
        - Equipos con software no identificado.
            C: Concienciar a los usuario y darles a conocer las normas recogidas en la política de conducta.

7.3 WiFi de acceso a invitados

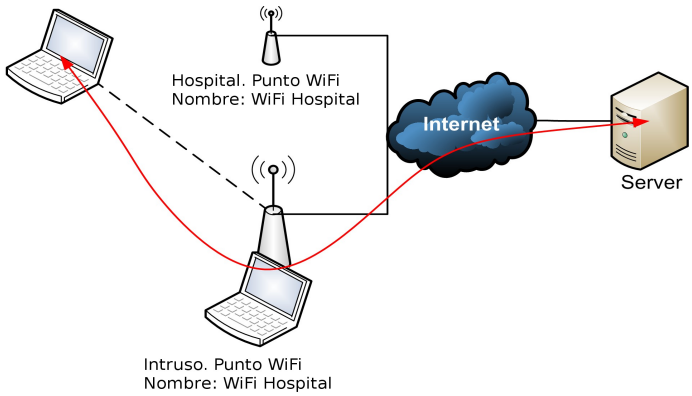
En este escenario nos situamos en un hospital donde tienen habilitada una red WiFi para proporcionar acceso a servicios de navegación por Internet a los usuarios del hospital. También se proporciona acceso a servicios propios del hospital.

Servicios ofrecidos:

- Acceso a Internet a través de conexión WiFi.
- Acceso a servicios limitados de la Intranet.

Riesgos y controles

- **Acceso a Internet a través de conexión WiFi**
    - Acceso no autorizado a la red WiFi.
        - C: Control de acceso de usuarios a través de portal cautivo.
    - Suplantación de punto de acceso (rogue AP).
        - C: Concienciación: Informar a los usuarios de las pautas a seguir para conectarse a la red WiFi.
    - Realización de acciones ilegales (cyberacoso, publicación de contenido con copyright, ...).
        - C: Concienciar a los usuario y darles a conocer las normas recogidas en la política de conducta.
        - C: Monitorización de la red.



    - Acceso a sitios maliciosos, de baja reputación, de contenido explícito y/o violento, etc.
        - C: Filtrado de contenidos.
        - C: Concienciar a los usuario y darles a conocer las normas recogidas en la política de conducta.
    - Ataques internos entre los equipos de la red local.

        - C: Configuraciones de red que eviten la comunicación directa entre equipos conectados a la misma red.
    - Conexión de equipos de usuarios a la red.
        - Equipos infectados
            - C: Acceso al servicio a través de portal cautivo.
            - C: Antivirus de red
        - Equipos con software no identificado.
            - C: Concienciar a los usuario y darles a conocer las normas recogidas en la política de conducta.
    - Realización de ataques anónimos.
        - C: Limitación de privilegios.
        - C: Limitación de recursos (ancho de banda, tiempo...).
        - C: Monitorización de la red.

- Acceso a servicios limitados de la Intranet
    - Acceso a servicios internos y redes no autorizadas.
        - C: Segregación de redes.
        - C: Control perimetral.
        - C: Monitorización de red.

8 CONCLUSIONES

Implementar un adecuado nivel de seguridad en las redes de acceso público de nuestra organización debe ser un elemento clave en la estrategia de seguridad definida. Cada servicio que se ofrezca deberá ser estudiado y sopesar pros y contra de ofrecerlo. Una incorrecta configuración de seguridad en este tipo de redes podría poner en riesgo nuestra red interna y los servicios críticos interconectados a ésta.

Es importante indicar que mantener y asegurar una red de acceso público es un proceso que necesita ser revisado, adaptado y mejorado continuamente, ya que en cualquier momento pueden surgir nuevos cambios en el escenario o nuevos riesgos que nos obliguen a replantearnos toda la implementación de las medidas y controles adoptados.

Sin embargo, es de suma importancia adecuarse siempre a las políticas de seguridad marcadas por nuestra organización y establecer los controles oportunos a fin de garantizar que han quedado cubiertos los máximos riesgos posibles.

9 DOCUMENTACIÓN DE REFERENCIA

- CERT-IF-2045-220812-Bastionado de Sistemas I
- CERT-IF-2718-260912-Bastionado_de_Sistemas_II
- SANS, 2002: Deploying Secure Public Kiosk Networks
- Li Zhao, Yun Zi . Kunming University of Science and Technology Library , 2013:The Network Security Management Problem of Library