GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 821

APÉNDICE II: NORMAS DE ACCESO A INTERNET NP10

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.02.23 09:28:35 +01'00'

FEBRERO 2018

ÍNDICE

1. OBJETIVO

1. El objetivo de la presente norma es regular el acceso a Internet por parte de los usuarios de los Sistemas de Información de la <<ENTIDAD>>, desde las distintas sedes de la <<ENTIDAD>> o a través de ellas, posibilitando la homogeneización de criterios dentro de sus unidades administrativas y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

   La presente Normativa deberá ser complementada, en su caso y en la medida oportuna, con la aplicación de las medidas de seguridad previstas en el Anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

2. Este documento se considera de uso interno de la <<ENTIDAD>> y, por tanto, no podrá ser divulgado salvo autorización de la <<ENTIDAD>>.

2. ÁMBITO DE APLICACIÓN

3. Esta Norma es de aplicación a todo el ámbito de actuación de la <<ENTIDAD>>, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información de la <<ENTIDAD>>.

4. La presente Norma **será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la <<ENTIDAD>>,** incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información de la <<ENTIDAD>>.

3. VIGENCIA

5. La presente Norma ha sido aprobada por la <<U/OC>> de la <<ENTIDAD>>, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la <<ENTIDAD>> pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

6. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la <<ENTIDAD>>.

7. Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa.

4. REVISIÓN Y EVALUACIÓN

8. La gestión de esta Norma corresponde a la <<U/OC>>, que es competente para:
   - Interpretar las dudas que puedan surgir en su aplicación.
   - Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
   - Verificar su efectividad.

9. Anualmente (o con menor periodicidad, si existen circunstancias que así lo

aconsejen), la <<U/OC>> revisará la presente Norma, que se someterá, de haber modificaciones, a la aprobación de la <<U/OC>> de la <<ENTIDAD>>.

10. La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

11. Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5. REFERENCIAS

12. *<<En este epígrafe se deben incluir aquellas referencias documentales que vengan a apoyar o completar esta Norma o que hubieren sido consideradas en su redacción.*

***Internas**:*

– ----
– ----
–

***Externas**:*

(Por ejemplo:

- *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.*
- *UNE - ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la información.*
- *UNE - ISO/IEC 27001:2007 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.*
- *ISO/IEC 9001:2000 Sistemas de gestión de la calidad.*
- *Documentos y Guías CCN-STIC.*
- *Etc.>>*

6. NORMAS PREVIAS

13. Las presentes "Normas de Acceso a Internet" complementa, en sus aspectos específicos, a la "NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DE LA <<ENTIDAD>>"[1], por lo que tal normativa general será de aplicación en los aspectos no señalados en aquella.

7. MOTIVACIÓN

14. Con carácter general, los usuarios de la <<ENTIDAD>> dispondrán de acceso a Internet como herramienta de productividad y conocimiento, para el desempeño de su actividad profesional.

15. Es necesario garantizar un uso adecuado de los recursos informáticos de acceso a Internet, por los siguientes motivos:

[1] Se recomienda que el organismo disponga de una Normativa General de Utilización de los Recursos y Sistemas de Información del <<ORGANISMO>>, del tipo descrito en el documento CCN STIC – 821 - NG00.

- **Seguridad**: Debido al riesgo de infección por software dañino (virus, troyanos, etc.).
- **Volumen del tráfico externo de datos:** Asegurando que el acceso a contenidos necesarios para la actividad profesional no se vea perjudicado por el tráfico generado por contenidos no vinculados con las competencias de la <<ENTIDAD>>.
- **Volumen del tráfico interno de datos:** Como consecuencia de contenidos descargados de la Web y su posterior almacenamiento. Esta situación aconseja también regular el tipo de ficheros cuya descarga y almacenamiento está permitido.
- **Ética**: Finalmente, es ineludible el compromiso que la <<ENTIDAD>> debe mantener con la sociedad, a la hora de vetar el acceso a contenidos que pudieran ser poco éticos, ofensivos o delictivos.

8. NORMATIVA

16. Con el despliegue de las TIC y, en particular, con el desarrollo de Internet como herramienta de comunicación global, se han extendido igualmente las amenazas que pueden poner en peligro los sistemas de información de las organizaciones.

17. En este sentido, la medida de seguridad [mp.per.2] del ENS señala:

> **Deberes y obligaciones [mp.per.2].**
>
> 1. Se informará a cada persona que trabaje en el sistema, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.
>
> a) Se especificarán las medidas disciplinarias a que haya lugar.
>
> b) Se cubrirá tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
>
> c) Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo, como posteriormente a su terminación.
>
> 2. En caso de personal contratado a través de un tercero:
>
> a) Se establecerán los deberes y obligaciones del personal.
>
> b) Se establecerán los deberes y obligaciones de cada parte.
>
> c) Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

18. Por tanto, para minimizar los riesgos derivados del uso de Internet, resulta necesario adoptar un conjunto mínimo de medidas de seguridad dirigidas a propiciar su correcto uso.

19. Tales medidas son:

- **Usar Internet para fines profesionales.** Internet es una herramienta más de las utilizadas por los usuarios de la <<ENTIDAD>>. Por ello, debe usarse de manera responsable y exclusivamente para fines profesionales[2].
- **No visitar páginas de contenido poco ético, ofensivo o ilegal.** No está permitido el acceso a páginas cuyo contenido pueda resultar ofensivo o atentar contra la dignidad humana. Análogamente, no se permite el acceso a páginas de contenido no adecuado, ilegal o poco ético.
- **No visitar páginas no fiables o sospechosas.** Para evitar posibles incidentes de seguridad, es aconsejable no visitar páginas que se consideren sospechosas de contener código malicioso.
- **Cuidar la información que se publica en Internet**. No se debe proporcionar información sobre la organización en foros, chats, etc., ya que podría ser utilizada de forma fraudulenta. En este sentido, está prohibido difundir sin autorización cualquier tipo de información no pública sobre el funcionamiento interno de la <<ENTIDAD>>, sus recursos, estructura, etc.
- **Observar las restricciones legales que sean de aplicación.** Antes de utilizar una información obtenida de Internet, los usuarios deberán comprobar en qué medida se halla sujeta a los derechos derivados de la Propiedad Intelectual o Industrial.
- **Realizar descargas sólo si se tiene autorización**. Las descargas indiscriminadas o sin autorización son uno de los orígenes más usuales de infección por código malicioso. Aunque la <<ENTIDAD>> decida no limitar técnicamente la capacidad para descargar archivos de audio o vídeo, los usuarios deberán tener en consideración que la descarga de estos archivos puede ir en detrimento del rendimiento de los recursos informáticos y, por ello, limitarán su descarga y reproducción al ámbito estrictamente profesional.
- **No descargar código o programas no confiables.** Es necesario asegurar la confiabilidad del sitio desde el cual se descargan los programas, utilizando siempre las páginas oficiales. Además, es necesario comprobar si es preciso el uso de licencia para utilizar las aplicaciones descargadas. Conviene que tales actividades sean acometidas, de manera exclusiva, por la <<U/OC>>.
- **Asegurar la autenticidad de la página visitada**. Cuando se vayan a realizar intercambios de información o transacciones es importante asegurar que la página que se visita es realmente la que dice ser. Es recomendable acceder a las páginas escribiendo y comprobando la dirección en la barra de direcciones del navegador y no a través de vínculos externos. Muchas suplantaciones de páginas Web muestran una página que es virtualmente idéntica a la página conocida por el usuario, incluso evidenciando un falso nombre en la barra de direcciones. Cuando la página web se encuentre autenticada mediante certificado digital, el usuario verificará su autenticidad.
- **Comprobar la seguridad de la conexión.** En general, la información transmitida por Internet no circula de manera cifrada. Sin embargo, en la transmisión de información sensible, confidencial o protegida es importante asegurar su cifrado. Una manera de asegurar la confidencialidad es comprobar que se utiliza

[2] Con las excepciones o precisiones que se señalen.

protocolo HTTPS en la comunicación en vez del protocolo estándar http (examinando la barra de direcciones). También debería aparecer un icono representando un candado en la barra del navegador. A través de dicho candado se puede obtener información sobre el certificado digital de identidad del sitio web visitado.

- **Cerrar las sesiones al terminar la conexión.** Es muy conveniente cerrar las sesiones al terminar la conexión o el intercambio de información, ya que en muchas ocasiones la conexión permanece abierta por defecto y no es suficiente con cerrar el navegador. Esto puede hacer que otros usuarios tengan acceso a las cuentas de los usuarios que no hubieren cerrado correctamente las sesiones. La mayoría de los sitios web disponen de una opción de "desconexión", "*logout*" o similar que conviene utilizar.
- **Utilizar herramientas contra código dañino.** El volumen de código dañino que circula en el ciberespacio es muy elevado y presenta multitud de aspectos diferentes[3]. Por tanto, es necesario disponer del adecuado abanico de herramientas que permitan una adecuada protección. El uso de un antivirus permanentemente actualizado es la primera de protección contra este tipo de ataques. Además de ello, es necesario configurar y usar adecuadamente cortafuegos, software específico contra programas espía (spyware), etc.
- **Mantener actualizado el navegador y las herramientas de seguridad.** Es imprescindible actualizar las herramientas de acceso a Internet (navegadores) y de seguridad (antivirus, cortafuegos, etc.) a las últimas versiones estables, siempre de conformidad con lo indicado y aprobado por la <<U/OC>>. Puesto que el código dañino se genera incesantemente, es muy importante actualizar las firmas de virus con la mayor frecuencia posible. Los sistemas deben estar configurados para realizar esta tarea de forma automática. Asimismo, es muy importante informar sobre cualquier problema que se detecte en este proceso.
- **Utilizar los niveles de seguridad del navegador**. Los navegadores Web permiten configuraciones con diferentes niveles de seguridad. Lo idóneo es mantener el nivel de seguridad "alto", no siendo recomendable utilizar niveles por debajo de "medio". Esto puede hacerse usando las herramientas disponibles en el navegador.
- **Desactivar las cookies.** Las cookies son pequeños programas que emplean los servidores Web para almacenar y recuperar información acerca de sus visitantes. (Por ejemplo, *quién*, *cuándo* y *desde dónde* se ha conectado un usuario). Estos programas se almacenan en el ordenador del usuario al visitar una página Web, pudiendo ser desactivados usando las herramientas disponibles en el navegador.
- **Eliminar la información privada.** Los navegadores Web almacenan información privada durante su utilización, tal como el historial de navegación, *cookies* aceptadas, contraseñas, etc.; información a la que podría acceder un atacante que se hubiera introducido en el sistema. Por tanto, es recomendable borrar esta información de manera periódica, usando las herramientas disponibles en el navegador.

[3] Véanse Informes de Ciberamenazas y Tendencias (varios años), del CCN.

- **No instalar complementos desconocidos**. Cuando se cargan ciertas páginas web, se muestra un mensaje comunicando la necesidad de instalar en el ordenador del usuario un complemento (*plug-in, add-on*, etc.) para poder acceder al contenido. Es muy recomendable analizar primero la conveniencia de instalar tal complemento y hacerlo, en cualquier caso, siempre desde la página del distribuidor o proveedor oficial del mismo.
- **Limitar y vigilar la ejecución de *Applets* y *Scripts***. Los *scripts* son un conjunto de instrucciones que permiten la automatización de tareas. Los a*pplets* son pequeñas aplicaciones (componentes de aplicaciones) que se ejecutan en el contexto del navegador Web. A pesar de que, en general, resultan útiles, pueden ser usados para ejecutar código malicioso y, por tanto, es recomendable limitar su ejecución.

9. CARACTERÍSTICAS DEL ACCESO A INTERNET

20. Por los motivos anteriormente expuestos, el acceso a Internet de los empleados de la <<ENTIDAD>> se realizará atendiendo a los siguientes criterios:

9.1. PUERTOS AUTORIZADOS

21. Se consideran puertos autorizados los siguientes:

Descripción del Puerto	Puertos autorizados
http (Servicios web estándar)	**p.ej. 80**
https (Servicio web seguro)	**p. ej. 443**
ftp (Servicio de transferencia de ficheros)	**p. ej. 21**
Servicios varios	**p. ej. 30080, 444, 8081, 8099, 8399**

22. En el caso de existir otros servicios que requieran puertos no estándar, se deberá comunicar a la <<U/OC>> para su estudio y autorización, en su caso.

9.2. CATEGORIACIÓN DE LAS PÁGINAS WEB

23. En el Anexo I se ofrecen las distintas categorías de páginas Web, con su descripción.

24. [En función de las necesidades y competencias de la <<ENTIDAD>>,] se detallan los siguientes grupos de acceso a tales categorías:

1	**Categorías no permitidas:**	**Anorexia – Bulimia, Azar, Chat (con intercambio de ficheros), Código malicioso, Construcción de explosivos, Drogas, Encuentros, Juegos, Logos/Ringtones, Modelos, Música, Pagar por navegar, Pornografía, Erotismo, Racismo, Rosa, Sectas, Servidores P2P, Violencia, Listas negras.**

2	**Categorías no permitidas, salvo autorizaciones especiales:**	Anonimizadores, DNS Services, Hackers, Servidores Mensajería Instantánea, VoIP, Spyware.
3	**Categorías permitidas:**	Resto de categorías señaladas en el Anexo I.

9.3. CATÁLAGO DE FICHEROS DE ACCESO RESTRINGIDO

25. Para minimizar los riesgos derivados de la descarga de ficheros, deberá considerarse restringido el acceso a los siguientes tipos de Ficheros (en el Anexo II se especifican las extensiones usuales que suelen poseer tales ficheros):

- Multimedia: Video, audio y *streaming*.
- Ejecutables.
- Imágenes de disco.
- De tamaño excesivo <<*por ejemplo, superior a 100 Mb*>>.

9.4. DISTRIBUCIÓN DE USUARIOS

26. Dentro de la <<ENTIDAD>> existen distintos niveles de usuarios, atendiendo a:

- Las categorías de los contenidos para los que tienen permiso de acceso.
- Los tipos de ficheros que tienen permiso de descarga.
- Limitación del tiempo de consulta.

27. Los usuarios se clasificarán en tres niveles de acceso, según la necesidad de utilización de Internet de los mismos.

28. (Por ejemplo):

Nivel de Acceso	Categorías Autorizadas	Limitación temporal	Descarga Ficheros	Especificaciones
1	3	NO	NO	La lista blanca se creará de forma manual bajo demanda de los usuarios previa autorización de <<U/OC>>. La lista blanca será de contenido útil para los trabajadores. (Quedan incluidas todas aquellas páginas categorizadas dentro de administraciones públicas)
2	3	NO	Sólo MULTIMEDIA	
3	**3 y 2**	**NO**	**Sólo MULTIMEDIA**	**Personal específicamente autorizado**

- El **nivel 1** tendrá acceso a páginas habituales sin restricción de tiempo y limitación de ficheros. Sin permiso para descargas.
- El **nivel 2** tendrá acceso a páginas habituales sin restricción de tiempo y limitación de ficheros. Descarga parcialmente permitida.
- El **nivel 3** tendrá acceso a más categorías que cualquier otro nivel. No se

aplican restricciones sobre ficheros, excepto a aquellos no recomendados por considerarse peligrosos.

9.5. PROPUESTA DE ASIGNACIÓN DE USUARIOS A NIVEL DE ACCESO

29. La asignación a un determinado nivel puede venir dada por el nivel profesional del usuario, de acuerdo con la siguiente tabla.

30. (Por ejemplo).

Tipo de Usuario	Nivel de acceso a Internet
Para todo el personal de la <<ENTIDAD>>	**1**
Especiales: p. ej. Gabinete de prensa	**2**
Especiales: personal informático y/o de seguridad con responsabilidad en temas de Internet	**3**

31. Cierto tipo de personal (por ejemplo: Subdirectores Generales, Delegados Provinciales, etc.) podrán solicitar de forma motivada, el cambio de nivel de acceso a Internet de un usuario mediante comunicación electrónica a <<U/OC>>.

9.6. SUSPENSIÓN DE DERECHOS DE ACCESO

32. Con carácter general, los usuarios de la <<ENTIDAD>> dispondrán de acceso a Internet como herramienta de productividad y conocimiento en el desempeño de su actividad profesional, por lo que la suspensión de los derechos de acceso sólo podrá realizarse mediante solicitud motivada y siempre que obedezca a algunas de las causas de mala utilización/abuso, recogidas en la "NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DE LA <<ENTIDAD>>"[4].

33. La suspensión del acceso a Internet finalizará cuando las razones objetivas que dieron lugar a la misma hubieren desaparecido

10. MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

34. Todos los usuarios de los recursos informáticos y/o Sistemas de Información de la <<ENTIDAD>> deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Norma, debiendo suscribirla.

[4] Se recomienda que el organismo disponga de una Normativa General de Utilización de los Recursos y Sistemas de Información del <<ORGANISMO>>, del tipo descrito en el documento CCN STIC – 821 - NG00.

35.

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [*personal de la <<ENTIDAD>>/empleado de la <<EMPRESA>>*], como usuario de recursos informáticos y sistemas de información de la <<ENTIDAD>>, declara haber leído y comprendido las Normas de Acceso a Internet de la <<ENTIDAD>> (*versión x*) y se compromete, bajo su responsabilidad, a su cumplimiento.

<<En _____, a____ de _____ de 20__>>

Organismo:	
Trabajador (Nombre y Apellidos):	
DNI número:	
Número de Registro de Personal:	
Firmado:	

Por la <<ENTIDAD>>: <<*Nombre y Apellidos*>>

DNI número: _____

Número de Registro de Personal: _____

ANEXO I: DESCRIPCIÓN DE CATEGORÍAS DE PÁGINA WEB

Categoría	Definición
Sector Público	Páginas Web de entidades de carácter público (Administraciones Públicas o sector Público Institucional), tales como Ministerios, Consejerías, Ayuntamientos, instituciones de la Unión Europea y, en general, cualquier dirección que aporte información referente a entidades de gobierno y administración de todo el mundo.
Anonimizadores	Páginas Web a través de las cuáles se evita el conocimiento por parte de terceros de las direcciones Web a las que se está accediendo.
Anorexia - Bulimia	Páginas Web dedicadas a promover e incitar la anorexia y la bulimia.
Arte y cultura	Páginas Web que aportan información relativa a las artes y las letras: museos, escultura, fotografía, literatura, etc.
Azar	Páginas Web desde donde poder acceder a casinos y bingos on-line. Se incluyen en esta categoría páginas donde poder realizar todo tipo de apuestas.
Bancos y Entidades Financieras	Entidades bancarias, Cajas de Ahorro, Compañías de Seguros, etc.
Banners	Cuadros de propaganda o publicidad insertados en páginas Web.
Blogs	Páginas gratuitas donde particulares publican en Internet, diarios, experiencias, comentarios, ideas, etc.
Buscadores	Páginas Web utilizadas para realizar búsquedas de contenidos en Internet (google.com, yahoo.com, altavista.com, etc.).
Chat	Páginas Web desde donde poder comunicarse con otros usuarios, en tiempo real.
Código dañino	Software introducido intencionadamente en un sistema con propósito malicioso o no autorizado.
Construcción de explosivos	Páginas Web relativas a la fabricación y manipulación de explosivos.
Compras	Páginas Web a través de las cuales se pueden realizar compras de productos y servicios varios.
Correo Web	Páginas Web donde poder enviar y recibir correos electrónicos.
Deportes	Páginas Web relativas a equipos e información deportiva.

Categoría	Definición
DNS Services	Categoría que abarca los casos de conexiones de equipos desde la red interna a equipos de usuarios en Internet, vía http, a un puerto destino configurable y variable, con la peculiaridad de que en el equipo de Internet se puede disponer de herramientas (tales como Remotely Anywhere, por ejemplo) que permiten el control total del equipo de Internet al usuario de la red interna y por tanto tener una vía de escape, ejecutando http, ftp, etc.
Drogas	Páginas Web que incitan al consumo de drogas o facilitan contactos / lugares donde poder adquirir estupefacientes. No se incluyen paginas informativas / preventivas sobre drogas.
Economía	Páginas Web con contenidos de bolsa, banca, inversiones financieras, seguros, etc.
Educación	Páginas Web de colegios, universidades, academias y cursos de formación en general.
Empleo	Páginas Web de ofertas y demandas de empleo. Se incluyen también las Webs de "head-hunters".
Encuentros	Páginas Web a través de las cuales se puede conocer a otras personas: hacer amigos, encontrar pareja, etc.
Entretenimiento	Páginas Web de información de ocio: películas, obras de teatro, libros, restaurantes, hobbies, etc. Contenidos, en general, sobre cómo emplear el tiempo libre, excepto los contenidos que pertenecen a azar, deportes, juegos y viajes.
Foros	Páginas Web de carácter temático donde se puede participar aportando opiniones personales.
Guías y callejeros	Páginas Web donde se incluyen callejeros de ciudades, información acerca de direcciones, números de teléfono, etc.
Hackers	Páginas Web donde poder encontrar software ilegal o procedimientos asociados con su uso.
Hosting domains	Páginas Web de empresas que alberga páginas Web, donde se pueden adquirir dominios de Internet.
Info	Páginas Web que en general aportan información útil, como situación del estado de las carreteras, predicciones meteorológicas, etc.
Informática	Páginas Web con información relativa a hardware, sofware, Internet, etc.

Categoría	Definición
Juegos	Páginas Web donde poder jugar "on-line" o descargar juegos de ordenador.
Jurídicas	Páginas Web que aportan información sobre temas legales.
Logos/Ringtones	Imágenes o Canciones (melodías monofónicas o polifónicas) que son descargadas por los usuarios de teléfonos móviles.
Modelos	Páginas Web donde se encuentren fotografías de modelos, total o parcialmente desnudos.
Música	Páginas Web para adquirir o descargar música o donde poder encontrar información relativa a cantantes y grupos musicales en general.
Pagar por navegar	Páginas Web que permiten ganar dinero en la red recibiendo correos, navegando por determinadas páginas, suscribiendo ofertas gratuitas, etc.
Páginas Personales	Páginas creadas en hosting especializados para ello, y que no están incluidas en otras categorías.
Pornografía	Páginas web de contenido pornográfico u obsceno. Se incluye el acceso a los chat donde se puede encontrar material de este tipo.
Erotismo	Páginas web de contenido erótico. Se incluye el acceso a los chat donde se puede encontrar material de este tipo.
Portales	Son sitios Web en los que se puede encontrar una amplia gama de contenidos: noticias, ocio, deportes, juegos, música, etc.
Prensa	Periódicos o revistas on-line.
Racismo	Páginas Web que abiertamente contengan contenidos de carácter xenófobo o inciten a comportamientos racistas o intolerantes por razón de cultura, raza, religión, ideología, etc.
Rosa	Páginas Web con contenidos relativos a personajes famosos. Además de contenidos como moda, perfumes, decoración, etc.
Salud	Páginas Web en las que se puede encontrar información de carácter divulgativo (no científico) acerca de enfermedades y sus remedios.
Sectas	Páginas Web de sectas peligrosas. No se incluirán aquellas organizaciones que, por legislación distinta entre países diferentes, sean consideradas sectas en unos países y asociaciones religiosas de pleno derecho en otras.

Categoría	Definición
Servidores P2P	Sitios donde se registran estos programas para dar el servicio y las páginas relacionadas con ellos.
Servidores Mensajería Instantánea	Sitios donde se registran estos programas para dar el servicio y las páginas relacionadas con ellos.
Sexualidad	Información y artículos sobre sexo, educación sexual, tendencias sexuales, etc., que no contienen pornografía.
Spyware	Páginas que contengan Spyware. Se considera Spyware al software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o consentimiento del propietario del ordenador.
Telecomunicaciones	Páginas Web que facilitan información acerca de temas de telefonía fija, telefonía móvil, conexión a internet, etc.
Viajes	Páginas Web de agencias de viajes, y aquellas con información turística acerca de ciudades, plazas hoteleras y medios de transporte.
Violencia	Páginas Web que abiertamente contengan contenidos de carácter violento, inciten a la violencia o hagan apología de ella.
VoIP	Voz sobre IP. Páginas desde las que se accede a aplicaciones que permiten la transmisión de voz en vivo a través de Internet utilizando los protocolos TCP IP.

ANEXO II: EXTENSIÓN DE FICHEROS DE ACCESO RESTRINGIDO

Descripción	Extensión	
Video (multimedia)	ASF: Windows Media AVI: BSPlayer BIK : RAD Video Tools DIV : DivX Player DIVX : DivX Player DVD : PowerDVD IVF : Indeo M1V : (mpeg) MOV : QuickTime MOVIE : (mov) MP2V : (mpeg) MP4 : (MPEG-4)	MPA : (mpeg) MPE : (mpeg) MPEG : (mpeg) MPG : (mpeg) MPV2 : (mpeg) QT : QuickTime QTL : QuickTime RPM : RealPlayer SMK : RAD Video Tools WM : Windows Media WMV : Windows Media WOB : PowerDVD
Audio (multimedia)	AIF : Winamp AIFC : Formato AIFF AIFF : Winamp AMF : Winamp ASF : Windows Media AU : Winamp AUDIOCD : AudioCD CDA : Winamp CDDA : AIFF Audio FAR : Winamp IT : Winamp ITZ : Winamp LWV: Microsoft Linguistically Enhanced Sound File MID : Winamp MIDI : Winamp MIZ : Winamp MP1 : Winamp MP2 : Winamp	MP3 : Winamp MTM : Winamp OGG : Winamp OGM : (Ogg) OKT : Winamp RA : Real Audio RMI : Winamp SND : Winamp STM : Winamp STZ : Winamp ULT : Winamp VOC: Winamp WAV: Winamp WAX: Acceso directo de audio de Windows Media WM : Windows Media WMA : Winamp WMV : Windows Media XM: Winamp XMZ: Winamp
Imágenes disco	MDS: Alcohol 120% CCD: Alcohol 120% / CloneCD CUE: Alcohol 120% / CDRWin (+.BIN) ISO: Alcohol 120% / Ahead Nero BTW: Alcohol 120% CDI: Alcohol 120% IMG: CloneCD (también de diskette y dibujo) NRA: Nero: CD audio	NRB:Nero: CD-ROM arranque NRE: Nero: CD EXTRA NRG: Ahead Nero NRH: Nero: CD-ROM híbrido NRI: Nero: CD-ROM ISO NRM: Nero: CD mixto NRU: Nero: CD-ROM UDF NRV: Nero: CD supervídeo CDC: Nero CD Cover

Descripción	Extensión	
Ejecutables	386: Controlador de dispositivo virtual BAT: Archivo por lotes MS-DOS BIN: Archivos binarios. CAB: Aplicaciones comprimidas. CFG: Configuraciones CMD: Secuencia de comandos de Windows NT COM: Aplicación MS-DOS DLL: Librería, extensión de aplicación DRV: Controlador de dispositivo DSN: Nombre del origen de datos DUN: Acceso telefónico de red EXE: Aplicación HT: HyperTerminal INF: Información de instalación INI: Opciones de configuración INS: Configuración de comunicaciones de Internet ISP: Configuración de comunicaciones de Internet JOB: Objeto de tarea KEY: Entradas de registro MSC: Documento de la consola común de Microsoft MSI: Paquete de Windows Installer	MSP: Revisión de Windows Installer NFO: MSInfo OCX: Control ActiveX OTF: Fuente OpenType PIF: Acceso directo a programa MS-DOS PMA: Archivo del Monitor de sistema PMC: Archivo del Monitor de sistema PML: Archivo del Monitor de sistema PMR: Archivo del Monitor de sistema PMW: Archivo del Monitor de sistema RDP: Conexión a Escritorio remoto REG: Entradas de registro SCF: Windows Explorer Command SCT: Windows Script Component SYS: Archivo de sistema VXD: Controlador de dispositivo virtual WSC: Windows Script Component WSF: Windows Script File WSH: Windows Script Host Settings File ZAP: Configuración de instalación de software
Streaming	FLV : Flas Video SPL : Shockwave Flash Object SWF : Shockwave Flash Object RAM : Streaming	