

Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1207

(04/2008)

SERIE X: REDES DE DATOS, COMUNICACIONES DE
SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Ciberseguridad

**Directrices para los proveedores de servicios
de telecomunicaciones acerca del riesgo de
programas espías y de software potencialmente
no deseado**

Recomendación UIT-T X.1207

UIT-T



RECOMENDACIONES UIT-T DE LA SERIE X
REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1207

Directrices para los proveedores de servicios de telecomunicaciones acerca del riesgo de programas espías y de software potencialmente no deseado

Resumen

La Recomendación X.1207 ofrece a los proveedores de servicios de telecomunicaciones directrices para abordar el riesgo que suponen posibles programas espías y software potencialmente no deseado. En esta Recomendación se promueven prácticas idóneas basadas en principios de claridad de la información y de consentimiento por parte del usuario, y de controles para los servicios web que alberga el proveedor de servicios de telecomunicaciones. En la Recomendación se desarrollan y promueven prácticas óptimas para los usuarios en materia de seguridad de los computadores personales, entre las cuales se encuentran la utilización en los sistemas del cliente de software contra los programas espías, antivirus, cortafuegos y las actualizaciones de seguridad.

Orígenes

La Recomendación UIT-T X.1207 fue aprobada el 18 de abril de 2008 por la Comisión de Estudio 17 (2005-2008) del UIT-T por el procedimiento de la Resolución 1 de la AMNT.

Palabras clave

Programas espías, seguridad de Internet, software engañoso, software potencialmente no deseado.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección <http://www.itu.int/ITU-T/ipr/>.

© UIT 2009

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

	Página
1 Alcance	1
2 Referencias	1
3 Definiciones.....	1
3.1 Software engañoso.....	1
3.2 Software potencialmente no deseado	1
3.3 Software espía	1
4 Siglas y acrónimos.....	1
5 Convenios	2
6 Descripción general	2
7 Objetivos.....	3
8 Software engañoso y software espía.....	3
9 ¿Por qué hay que preocuparse por los efectos del software engañoso y del software espía?	3
10 Recomendaciones	4
11 Directrices para los proveedores de servicios de telecomunicaciones (TSP).....	4
11.1 Gestión de riesgos para la seguridad de la información en las empresas.....	4
11.2 Requisitos de seguridad para los servicios de alojamiento de páginas web...	6
11.3 Orientación para la seguridad de los usuarios	8
Apéndice I – Otros recursos.....	10
I.1 Referencias en línea sobre seguridad y antídotos contra el software espía....	10
Bibliografía	13

Recomendación UIT-T X.1207

Directrices para los proveedores de servicios de telecomunicaciones acerca del riesgo de programas espías y de software potencialmente no deseado

1 Alcance

Esta Recomendación forma parte de un conjunto de directrices publicadas por el UIT-T con miras a mejorar el estado de la ciberseguridad. Cubre las prácticas y los requisitos básicos que han de seguir los proveedores de servicios de telecomunicaciones (TSP, *telecommunication service providers*) y los usuarios, concentrándose en aspectos relacionados con el software espía y otro software potencialmente no deseado, que puede ser malicioso y/o engañoso. En esta Recomendación se entiende por proveedores de servicios de telecomunicaciones los TSP que ofrecen servicios relacionados con Internet, especialmente el alojamiento de sitios web de empresas y el acceso Internet de usuarios.

2 Referencias

Ninguna.

3 Definiciones

La expresión software espía (*spyware*) se utiliza de una manera muy general para referirse a numerosas formas de software que presentan ciertos comportamientos violatorios de la privacidad que no son solicitados por el usuario. En aras de la coherencia, se suministra a continuación una definición del software espía y del software engañoso.

3.1 Software engañoso

Software que realiza actividades en el computador de un usuario sin antes: 1) informarle exactamente qué va a hacer en él, ni 2) preguntarle si acepta que lo haga. Algunos ejemplos de software engañoso son los programas que secuestran las configuraciones o los programas de usuario, provocando una serie interminable de ventanas de publicidad que el usuario no puede interrumpir fácilmente.

3.2 Software potencialmente no deseado

Se refiere a varias formas de software engañoso, incluidos el software malintencionado, por ejemplo los virus, los gusanos de red y los caballos de Troya, y el que no es malintencionado pero tiene características de software engañoso y espía.

3.3 Software espía

Se define en esta Recomendación como un tipo particular de software engañoso que recolecta en un computador información personal del usuario. Esta información puede incluir la lista de sitios web más visitados, o información más delicada, como las contraseñas.

4 Siglas y acrónimos

En esta Recomendación se utilizan las siguientes siglas y acrónimos:

EIEI	Equipo de intervención en caso de emergencia informática
EIII	Equipo de intervención en caso de incidente informático
FSI	Fabricante de software independiente

SGSI	Sistema de gestión de la seguridad de la información
SGSI-T	Sistema de gestión de la seguridad de la información – Requisitos para las telecomunicaciones
SQL	Lenguaje de indagación estructurado (<i>structured Query language</i>)
TIC	Tecnologías de la información y la comunicación
TSP	Proveedor de servicios de telecomunicaciones (<i>telecommunication service provider</i>)
URI	Identificador uniforme de recursos (<i>uniform resource identifier</i>)

5 Convenios

Ninguno.

6 Descripción general

El auge de Internet ha dado lugar a nuevas actividades comerciales y ha generado múltiples beneficios a los consumidores, tanto en sus hogares como en su trabajo. El carácter inherentemente abierto de Internet, unido a la interconectividad y la velocidad de acceso que proporciona, lo han transformado también en una plataforma eficaz para las comunicaciones de los usuarios y las empresas, al igual que a los efectos de los mercados de masas. Recientemente, el carácter abierto de Internet, su facilidad de comunicación y su conectividad, han sido utilizados por ciberdelincuentes y por compañías sin escrúpulos, valiéndose de diversos tipos de software malintencionado, para obtener beneficios financieros u otros propósitos ilegales.

El software espía y engañoso es uno de los problemas de seguridad cada vez más omnipresentes, que causa pérdidas importantes de productividad y hace que los usuarios pierdan confianza en los negocios legítimos a través de Internet.

Con frecuencia, varias de las partes implicadas, especialmente los reguladores y los clientes empresariales, exigen a los proveedores de servicios de telecomunicaciones que proporcionen servicios Internet seguros a los usuarios (incluyendo los domésticos y los empresariales). Cuando se detecta que un sitio web localizado en la red de un TSP alberga contenidos malintencionados, incluidos los software espías o engañosos, que afectan la seguridad de los sistemas de los computadores de los usuarios, se solicita la ayuda del TSP, y toda aparición prolongada o recurrente de dichos incidentes afecta la confianza en la capacidad del TSP para ofrecer servicios seguros, con lo cual los consumidores podrían migrar hacia otros proveedores.

Desde una óptica reglamentaria, los reguladores de varios países están solicitando garantías a los TSP sobre las medidas de seguridad que hayan tomado, y les están sugiriendo que mejoren la asesoría que ofrecen a los clientes en materia de utilización segura de Internet.

Teniendo en mente los cambios mencionados en la esfera de seguridad del entorno Internet, es fundamental que los TSP adopten una serie de prácticas idóneas, que puedan ser reconocidas como una base mínima en el sector¹, que garantice la prestación segura de los servicios Internet del TSP, y fomenten unas prácticas al respecto que deban seguir los usuarios de sus redes. Al poner en marcha las prácticas óptimas, el TSP demostrará a los reguladores y a los usuarios que se acoge a las prácticas óptimas aceptadas en el sector, mejorando, o manteniendo, la confianza de ambos en la seguridad de sus redes y servicios.

¹ Actualmente, no existe una base mínima de prácticas idóneas y con esta Recomendación se pretende colmar dicha carencia.

7 Objetivos

Esta Recomendación tiene como fin:

- 1) fomentar la utilización de prácticas idóneas que se articulen en principios de claridad de la información, consentimiento del usuario y controles de usuario para los servicios web; y
- 2) fomentar prácticas idóneas (a través de los TSP) en materia de la utilización segura por parte de los usuarios residenciales de los computadores y de Internet, incluyendo el empleo de antivirus, programas contra el software espía, cortafuegos personales y actualizaciones automáticas de seguridad.

8 Software engañoso y software espía

Los programas de software engañoso (incluidos los espías) se distinguen de las aplicaciones legítimas porque en ellos no se notifica al usuario ni éste tiene poder de decisión. Es importante anotar que si hubiera transparencia, si el usuario tuviera el control y pudiera dar su autorización, muchas de las funciones ejecutadas por el software engañoso/espía podría producir beneficios para el usuario. Por ejemplo, es posible que dichos programas permitan la personalización de servicios, activen cambios de configuración aprobados por el usuario y presenten publicidad aprobada, lo que a su vez podría permitir subsidiar el costo de ciertos servicios de gran valor añadido, tales como el correo electrónico. En síntesis, el software engañoso no es tanto un problema tecnológico como uno provocado por comportamientos engañosos o fraudulentos.

Tanto en el ámbito mundial como en el local, el software engañoso y el software espía se han convertido en asuntos de primera línea para los gobiernos, el sector y los consumidores, que traspasan la esfera de asuntos de "política TIC". Si bien es evidente que el software engañoso se vale de Internet y de los computadores como sus medios, sigue siendo sobre todo un problema de protección del consumidor que se deriva de un comportamiento engañoso.

9 ¿Por qué hay que preocuparse por los efectos del software engañoso y del software espía?

Desde el punto de vista del consumidor, este tipo de software perjudica la experiencia computacional y/o en línea del usuario (a veces, hasta el punto de hacer inutilizable el computador) y genera un sentimiento de frustración y una impresión de que el usuario "ha perdido el control". No es una exageración decir que, como resultado del software engañoso, buena parte de los usuarios residenciales pueden perder casi todos los beneficios potenciales de Internet y de la informática.

Aunque el software engañoso tiene un efecto evidente sobre los consumidores, también es un problema para la mayoría de las empresas del sector de las TIC. De una parte, numerosos consumidores atribuyen erróneamente los problemas de utilización del computador a fallas de los fabricantes de equipos y de los productores de software, lo cual perjudica la reputación de éstos y desmejora la imagen que los consumidores tienen de sus productos. Los problemas provocados por el software engañoso también generan costos innecesarios, representados en millones de dólares gastados en llamadas a los centros de ayuda al usuario, para los sectores de software y de equipos.

Como se indicó en la cláusula 6, los TSP también deben preocuparse por el software engañoso y el software espía, puesto que entre los sitios web que acogen puede haber algunos utilizados por compañías sin escrúpulos y ciberdelincuentes para engañar con ese tipo de software a sus abonados, tras lo cual éstos llaman al TSP para pedirle ayuda. Los reguladores y los usuarios esperan que los TSP pongan en práctica medidas de protección adecuadas contra dichos problemas. De no hacerlo, se ven afectadas su reputación y la confianza de los usuarios.

10 Recomendaciones

La manera más eficaz de enfrentar el software espía conlleva probablemente una combinación de varias estrategias, en las que participan las partes interesadas, a saber:

- la utilización de prácticas idóneas de la industria, con la colaboración de todos los actores clave, a fin de identificar y hacer frente al software espía y a todo otro software no deseado;
- una amplia campaña de información del usuario, que le proporcione una fuente fidedigna de información acerca de cómo suprimir y evitar el software espía y otro software no deseado;
- la utilización de soluciones tecnológicas novedosas para la protección de los usuarios contra el software espía y otro software potencialmente no deseado, y para garantizar la entrega oportuna de actualizaciones; y
- la promulgación de una legislación y su aplicación por parte de las autoridades, con la colaboración de la industria, para desalentar el desarrollo de software engañoso y software espía.

Estas directrices se concentran en el suministro de prácticas idóneas para la industria y en el diseño de una amplia campaña de información del usuario, con el fin de asesorar a los TSP para que puedan desempeñar una función activa en la prevención del software engañoso y del software espía.

11 Directrices para los proveedores de servicios de telecomunicaciones (TSP)

Con miras a resolver los problemas planteados por el software engañoso y el software espía, estas directrices se concentran en tres aspectos principales, a saber, la gestión de la seguridad interna del TSP propiamente dicho; los requisitos de seguridad que el TSP debe especificar a los clientes a los que les presta el servicio de alojamiento de servicios web; y consejos de seguridad útiles para los usuarios (o abonados) de los servicios de acceso a Internet. Las recomendaciones se dividen a su vez en tres subsecciones:

- a) Gestión de riesgos para la seguridad de la información en las empresas.
- b) Requisitos de seguridad para los servicios de alojamiento de servicios web.
- c) Consejos en materia de seguridad para los usuarios.

11.1 Gestión de riesgos para la seguridad de la información en las empresas

11.1.1 Sistema de gestión de la seguridad de la información

En las empresas debe existir un sistema formal de gestión de la seguridad de la información que permita la identificación y la gestión de los riesgos relacionados con la seguridad de la información que afectan a los TSP. En [b-UIT-T X.1051] se ofrece la ayuda necesaria y las prácticas idóneas para poner en funcionamiento dicho sistema.

Un aspecto clave que han de tener en cuenta los TSP al implementar un ISMS-T es que hay que asegurarse de que, en tanto que organización, poseen un sistema que permita identificar, evaluar, tratar y gestionar permanentemente riesgos para la seguridad de la información, relacionados con su prestación de servicios en Internet, bien sea directamente a los usuarios/abonados o bien a los clientes a través de servicios web que ellos alojen.

Gracias a los procesos para la gestión permanente de riesgos que tiene el ISMS-T, los TSP conocerán mejor su perfil de riesgo y podrán demostrar a los reguladores y a otras partes interesadas que sus redes y servicios son seguros.

Asimismo, los TSP pueden optar por obtener la certificación formal de conformidad con las Recomendaciones ISMS-T, con arreglo al esquema de certificación ISO/CEI 27001.

Como parte de la implementación del ISMS-T u otro sistema pertinente de gestión de la seguridad de la información, los TSP también deben crear un sistema de supervisión de incidentes que afectan la seguridad y poner en marcha una metodología de respuesta a ellos, y coordinar dichas actividades de respuesta a los incidentes con los equipos de intervención en caso de incidente informático (EIII) o equipos de intervención en caso de emergencia informática (EIEI) de las organizaciones en el país. Las actividades de respuesta a los incidentes y las emergencias deben conllevar la supervisión y la evaluación del estado de los usuarios y de los sitios web alojados en las redes del TSP, y proporcionar asesoría a las partes afectadas para que actúen eficientemente ante los incidentes de seguridad.

11.1.2 Suministro de productos seguros

Es posible que algunos TSP desarrollen² sus propias barras de herramientas (*toolbars*), programas para establecer la conexión a Internet (*diallers*) o software de todo tipo para proporcionar servicios de valor añadido a los usuarios o facilitarles el acceso a los servicios Internet. De ser así, se ha de informar claramente al usuario y solicitarle su acuerdo acerca de la política de programación del TSP, su política de privacidad, y proporcionarle los medios para que modifique en el futuro las condiciones de aceptación o pueda considerar todo aspecto relacionado con la política o las prácticas. Cuando se utilice este tipo de acuerdo, el TSP debe verificar que los usuarios lo firmen y que la versión sea la correspondiente.

Los TSP también tienen que suministrar información acerca del comportamiento de su software y evaluar si en algunos casos dichos programas se pueden considerar como engañosos o espías. Si fuere el caso, el TSP debe contratar asesores calificados que evalúen si se puede contrarrestar este comportamiento utilizando los remedios contra el software espía que existen en el mercado, y adoptar prácticas idóneas, a fin de que el software que proporciona a los usuarios no sea catalogado como espía, o como publicidad forzosa, por los proveedores de servicios contra dicho tipo de software. La mayoría de los proveedores de estos antídotos contra el software espía publican los criterios mediante los cuales clasifican un programa como espía³.

Los TSP deben firmar digitalmente los códigos binarios para facilitar la tarea de identificación de la fuente por parte de los proveedores de antídotos, con lo cual el software de los fabricantes de software independientes (FSI) que siguen rigurosa y sistemáticamente las prácticas recomendadas podrá ser clasificado como seguro incluso antes de ser analizado.

Si los TSP llegasen a encontrar técnicas de software que permitieran disminuir el problema del software espía, deberían colaborar con el proveedor para su difusión.

11.1.3 Supervisión de la red y respuesta en caso de incidente

Los TSP suelen emplear la supervisión de red para garantizar la fiabilidad y la calidad de sus servicios de red. Esta capacidad también puede servir para identificar condiciones excepcionales de tráfico y detectar la aparición de actividades malintencionadas en la red. En general, los TSP deben:

- Entender el tráfico de la red – qué es normal, qué es anormal.
- Utilizar la herramienta de gestión de red para identificar picos de tráfico y tráfico/puertos "inusuales", y garantizar que se cuenta con los medios para señalar las causas de los problemas y actuar en función de ellas.
- Verificar la capacidad de respuesta antes de que ocurran eventos reales. Mejorar las técnicas, los procesos y las herramientas de respuesta, basándose en pruebas periódicas.

² Bien sea internamente o a través de otro proveedor.

³ La coalición contra el software espía (*AntiSpyware Coalition*), en la que participan numerosas empresas, también tiene un conjunto de definiciones y criterios, que publica en su sitio web. En el apéndice I se encuentra más información al respecto.

- Comprender bien el comportamiento de cada una de las partes – si un usuario normal y poco activo empieza a utilizar el 100% de la banda disponible, es posible que haya que aislarlo hasta que se encuentre la razón para ello. El aislamiento puede ser un remedio contra la propagación de software malintencionado (*malware*), aunque en algunos casos tal vez se requiera el consentimiento del usuario o la actualización de las condiciones de servicio.

11.1.4 Ayuda al usuario e intensificación del problema

En general, los TSP tienen un servicio de ayuda al usuario que responde a sus preguntas y les proporciona asistencia técnica. El aumento de la presencia de software malintencionado en Internet hará que los TSP reciban cada vez más informes relacionados con infecciones causadas por software espía y malintencionado y otros temas afines. Dicha información es importante y útil para los proveedores, pues les permite evaluar riesgos, y les proporciona las actualizaciones de las herramientas necesarias para suprimir o inhabilitar eficazmente todo software de este tipo que sea detectado. En este orden de ideas, los TSP han de establecer contacto con los proveedores de seguridad y presentarles los informes de seguridad y las muestras de software malintencionado pertinentes, a fin de que puedan actuar a tiempo – especialmente si se trata de amenazas que prevalecen. La mayoría de los proveedores tienen una lista de distribución de correo-e en la que se reciben dichos informes/muestras, que luego analizan y resuelven. Por ejemplo, véase el cuadro I.1.

11.1.5 Cómo mantenerse al día sobre los desarrollos más recientes

Al poner en funcionamiento el ISMS-T, para gestionar los riesgos de seguridad de la información en la empresa y garantizar la conformidad con las prácticas idóneas del sector y estar al día acerca de las vulnerabilidades y ataques más recientes, el TSP ha de participar en los foros comunitarios o del sector que sean relevantes, con el fin de compartir información acerca de sus métodos y aprender de los otros proveedores.

NOTA – Puede encontrarse más información en el apéndice I.

11.2 Requisitos de seguridad para los servicios de alojamiento de páginas web

La mayoría de los TSP ofrece, como parte de sus actividades comerciales, servicios de alojamiento de páginas web en sus redes y centros de datos. Dichos servicios llegan a los usuarios/consumidores/pequeñas empresas a través de los abonados al servicio de alojamiento de páginas web, quienes los "reempacan" y los revenden. Si estos abonados al servicio de alojamiento tienen servidores inseguros, o en ellos hay contenido malintencionado, la seguridad de los usuarios se verá afectada. Por lo tanto, es importante que los TSP inviten a los abonados al servicio de alojamiento a que cuenten con un mínimo de seguridad y que adopten unas prácticas idóneas, como parte del acuerdo de prestación de servicios.

Las condiciones del acuerdo deben:

- a) Incluir avisos claros, en los que se describan las prácticas en materia de seguridad, de privacidad del sitio web y de recolección de datos, y el comportamiento de todo software (por ejemplo, un objeto de ayuda en el navegador) que el sitio web pueda distribuir y ejecutar en el computador del usuario o en el entorno del navegador web.
- b) Permitir que se solicite el consentimiento del usuario, quien puede manifestar su acuerdo o desacuerdo con las condiciones de servicios descritas en los avisos. De esta manera, queda a discreción del usuario decidir si acepta o no las condiciones.
- c) Incluir controles de usuario, con lo cual los usuarios pueden modificar sus parámetros o dejar de aceptar, en cualquier momento, las condiciones del acuerdo inicial.

Las condiciones son importantes para garantizar que los usuarios conocen claramente el comportamiento y las prácticas del sitio web, en lo que toca a la seguridad y la privacidad del usuario. Estas condiciones han de establecerse con la ayuda de abogados expertos, de tal manera que los TSP estén cubiertos contra posibles demandas de usuarios que hayan sufrido pérdidas o daños específicos causados por contenido malintencionado o políticas o prácticas del sitio web poco claras.

Además de las disposiciones para la protección y la salvaguarda de la privacidad en el sitio web, los TSP han de exigir a los sitios web alojados en su red que apliquen un conjunto de prácticas óptimas en materia de seguridad, al nivel de aplicación, antes de que puedan entrar en línea. Las condiciones han de ser, aunque no se limitan a:

- a) Orientación para el desarrollo de sitios web seguros y prácticas de desarrollo de software, incluidos:
 - i) la presentación de avisos cortos de privacidad, que proporcionen un resumen claro y conciso de una página (en términos simples) de las prácticas principales de la empresa en materia de privacidad en línea. Los usuarios podrán, gracias a estos avisos, tener más elementos de juicio para juzgar si permiten que se comparta la información en línea que les concierne. Los avisos cortos han de ser conformes con todos los requisitos reglamentarios y deben suministrar hipervínculos a declaraciones jurídicas completas y otras informaciones pertinentes, para que los consumidores que así lo quisieran pudieran leer la versión completa. Un aviso único permite que los consumidores tengan una experiencia coherente con todos los servicios del proveedor, con las mismas normas de protección de la privacidad e iguales expectativas con muchos sitios web;
 - ii) el manejo seguro de las "cookies";
 - iii) la validación y manejo seguros de las entradas de datos, para evitar ataques del tipo inyección SQL. Basándose en que con cada vez más frecuencia se utilizan sitios web muy visitados para la distribución de códigos malintencionados, habrán de realizarse validaciones de entrada y salida del contenido activo y el contenido dinámico;
 - iv) la utilización segura de *scripts* en las páginas web, para evitar ataques del tipo inyección de código a través de *scripts* ejecutados en otros sitios (*cross-site scripting*);
y
 - v) el análisis y la verificación de la seguridad del software.

La infraestructura para el alojamiento de páginas web del TSP incluye también las siguientes medidas de protección de los servidores web contra el acceso no autorizado y la amenaza de contenidos malintencionados, tales como los engañosos y espías:

- b) Se debe configurar el servidor web, incluyendo sus sistemas operativos subyacentes, con arreglo a una configuración básica de seguridad. Dicha configuración ha de incluir una definición apropiada de usuario del servidor web y sus diferencias con el administrador, instaurar controles de acceso en los programas y directorios de sistemas y ficheros, y activar las pistas de auditoría de seguridad, en particular para eventos de seguridad y otros fallos del sistema. Además se recomienda instalar en el servidor un sistema mínimo para reducir el vector de ataque.
- c) Hay que utilizar un sistema de pruebas y despliegue de actualizaciones de seguridad, y garantizar que el sistema operativo y las aplicaciones del servidor dispongan cuanto antes de las nuevas actualizaciones.
- d) Se debe contar con una supervisión del desempeño en materia de seguridad del servidor web, a través de un análisis periódico de las pistas de auditoría de seguridad.
- e) Hay que utilizar antivirus y antídotos contra el software espía en el servidor.

- f) Es necesario analizar regularmente todo el contenido alojado y telecargado utilizando definiciones actualizadas. Ha de ser posible identificar a un determinado fichero como software espía o malintencionado aunque no haya sido detectado a través de las definiciones en vigor, como resultado de una información imperfecta.
- g) Se debe llevar a cabo una prueba periódica de la seguridad de los sitios web, para garantizar que ésta se mantiene adecuadamente y que no ha sido amenazada.

Con el fin de poder hacer aplicar estas medidas, en particular las que tienen que ver con la seguridad del sitio web, los TSP deberían incorporar estas disposiciones en sus condiciones de servicio.

11.3 Orientación para la seguridad de los usuarios

11.3.1 Orientación y suministro de información al usuario

Orientación sobre cómo permanecer seguro en línea. Los TSP pueden proveer la orientación directamente o remitir al usuario a sitios de ayuda en los que puede encontrar el contenido pertinente. Es clave informar al usuario sobre cómo contribuir a que Internet sea más seguro. Entre las campañas o actividades de orientación se cuentan las siguientes:

- a) envío de boletines periódicos de seguridad (mensuales, por ejemplo) en los que se ofrezca asesoría sobre técnicas específicas de seguridad (por ejemplo, cómo escoger una buena contraseña) y actualizaciones sobre tendencias en materia de seguridad; y suministro de avisos acerca de difusiones relacionadas con la seguridad y otros vídeos a la carta, difusiones de audio e información de seguridad disponibles en el portal web del TSP u otros proveedores de contenidos de seguridad;
- b) difusión directa de vídeos de información a la carta sobre temas de seguridad y/o transmisiones a través de la web de una variedad de tópicos de seguridad, con el fin de mejorar sus prácticas y conocimiento en estos temas;
- c) mantener una columna sobre la seguridad en la edición en papel del boletín periódico del TSP que se envía a la residencia u oficina del usuario, con énfasis en contenidos o eventos claves de seguridad; y
- d) realización de talleres o exposiciones anuales, o con otra periodicidad, sobre seguridad para los usuarios, probablemente en colaboración con otros actores del sector, proveedores y gobiernos.

11.3.2 Medidas técnicas de seguridad en el plano de usuario

Como parte de las campañas de información y orientación del usuario contra el software engañoso y el software espía, el TSP debe aconsejar a los usuarios que empleen medidas técnicas de seguridad apropiadas para proteger sus sistemas contra los ataques conocidos. Las medidas de protección mínima son:

- a) utilización de los sistemas operativos más recientes, en los que se hayan instalado los parches de seguridad más actualizados;
- b) utilización de herramientas antivirus y contra el software espía. De ser posible, el TSP debe colaborar con proveedores de seguridad de confianza⁴, mediante la oferta de sus servicios como parte del abono al TSP, de tal manera que las medidas de seguridad están disponibles desde el mismo instante de la firma de la suscripción o de su renovación;
- c) permitir el bloqueo de las ventanas intempestivas. Los navegadores web y las barras de herramientas más utilizados ya han incorporado esta capacidad, gracias a la cual se puede

⁴ Los proveedores de seguridad de confianza pueden ser socios de los TSP y/o proveedores cuyos productos y servicios hayan sido evaluados y cumplen con los requisitos y políticas de seguridad de los TSP.

evitar que sitios web malintencionados presenten ventanas que contengan software engañoso o espía que pueda valerse de debilidades del sistema de navegación, o utilizar la ingeniería social, para engañar a los usuarios, obligándolos a telecargarlos e instalarlos en sus sistemas. Debe anexarse una lista de herramientas recomendadas para bloquear las ventanas intempestivas, alentar su utilización y suministrar orientación acerca de cómo hacerlos funcionar y cómo permitir las ventanas provenientes de sitios en los que confía el usuario;

- d) utilizar un cortafuegos personal. Se trata de otra herramienta importante para controlar los servicios de red que acceden al sistema del usuario y viceversa. Algunos de los sistemas operativos más recientes incluyen dichos cortafuegos personales. Si bien estas herramientas se habilitan por defecto, los usuarios u otras aplicaciones pueden inhabilitarlos, con lo cual se exponen a problemas de seguridad de red indeseables. Los TSP han de alentar la utilización de funciones cortafuegos personales, y/o sugerir el empleo de productos de terceras partes personal que hayan sido evaluados por, y en los que confíe el TSP, e informar y ayudar a los usuarios para que mantengan una seguridad mínima en sus sistemas;
- e) permitir las actualizaciones automáticas. Mientras que las medidas técnicas mencionadas *supra* contrarrestan la mayoría del software malintencionado en sus niveles respectivos, no son eficaces contra la explotación de las vulnerabilidades existentes en sistemas operativos y productos de aplicación. Para evitar esto último, se debe contar con una función de actualización del sistema operativo, y que sea ofrecida por aplicaciones en las que confíe el usuario (por ejemplo, productos evaluados antivirus y contra el software espía que provengan de una tercera parte de confianza). De esta manera se garantiza que el sistema cuente con los parches más recientes tan pronto se dispone de ellos, con lo cual se disminuye el lapso de tiempo durante el cual puede tener éxito un ataque.

En el apéndice I se presenta una lista de referencias y recursos en línea que puede servir para llevar a la práctica las recomendaciones efectuadas en esta Recomendación.

Apéndice I

Otros recursos

(Este apéndice no forma parte integrante de esta Recomendación)

I.1 Referencias en línea sobre seguridad y antidotos contra el software espía

Existen varios sitios web que pueden servir como referencia y ser aprovechados para obtener más información relacionada con la seguridad en Internet, a saber:

- **Coalición contra el software espía (ASC, *Anti-spyware Coalition*)** (<http://www.antispywarecoalition.org/>) – Grupo que se dedica a alcanzar el consenso acerca de las definiciones y prácticas idóneas en materia de software espía y otras tecnologías potencialmente no deseadas. La ASC se compone de proveedores de antidotos contra el software espía, instituciones académicas y grupos de consumidores, y tiene como fin reunir diferentes perspectivas del problema del control del software espía y otras tecnologías potencialmente no deseadas.
- **Be Web Aware** (<http://www.bewebaware.ca>) – Programa nacional de información pública bilingüe acerca de la seguridad en Internet, cuyo fin es garantizar que los jóvenes canadienses se beneficien de Internet de una manera segura y responsable mientras estén en línea.
- **Centro para la utilización segura y responsable de Internet (*Center for Safe and Responsible Internet Use*)** (<http://csriu.org>) – Organización que proporciona servicios de divulgación de temas relacionados con la utilización segura y responsable de Internet.
- **Childnet International** (<http://www.childnet-int.org>) – Organización sin ánimo de lucro que actúa en colaboración con otras organizaciones de todo el mundo para que Internet sea un lugar seguro y excelente para los niños.
- **ECPAT** (<http://www.ecpat.net>) – Red compuesta por organizaciones e individuos que tiene como fin eliminar la explotación sexual de los niños.
- **GetNetWise** (<http://www.getnetwise.org>) – Servicio público ofrecido por una coalición de empresas y de organizaciones de interés público del sector Internet que propenden porque los usuarios puedan estar a "un sólo clic" de distancia de los recursos necesarios para tomar decisiones fundamentadas acerca de la utilización de Internet por su parte y la de sus familias.
- **Global Infrastructure Alliance for Internet Safety (GIAIS)** (<http://www.microsoft.com/security/msra/default.aspx>) – Alianza conformada por los principales proveedores mundiales de servicios Internet, creada para mejorar la seguridad en la web, hacer frente de una manera coherente a una amplia gama de amenazas e identificar y mitigar las vulnerabilidades existentes.
- **INHOPE** (<http://inhope.org>) – Asociación internacional que provee servicios de ayuda (*hotlines*) acerca de Internet, con miras a contrarrestar contenidos ilegítimos y hacer de Internet algo más seguro.
- **Grupo para la seguridad en Internet (ISG, *Internet safety group*)** (www.netsafe.org.nz) – El sitio web de NetSafe es la sede en línea del ISG de Nueva Zelandia y de "Héctor el protector".
- **International Centre for Missing & Exploited Children** (<http://www.icmec.org>) – Agencia mundial que promueve la seguridad y el bienestar de los niños, a través de activismo, desarrollo de políticas y coordinación multinacional.

- **Interpol** (<http://www.interpol.int>) – Organización internacional de policía que permite la colaboración de los cuerpos de policía de diferentes países, y asesora a las organizaciones, las autoridades y los servicios cuya misión sea prevenir o combatir el delito internacional.
- **iSafe** (<http://www.isafe.org>) – Organización líder en materia de información sobre la seguridad en Internet; incluye contenidos que permiten a estudiantes, profesores, padres, autoridades, y adultos interesados hacer de Internet un lugar más seguro.
- **Microsoft Security At Home** (<http://www.microsoft.com/protect>) – Información y recursos que sirven para ayudar al público a proteger sus computadores, protegerse ellos mismos y sus familias.
- **National Council for Motherhood and Childhood** (<http://www.nccm.org.eg>) – Organización egipcia dedicada a proteger a la infancia y a las madres de familia, desde una óptica de sus derechos.
- **Net Family News** (<http://netfamilynews.org>) – Servicio público sin ánimo de lucro que tiene un foro y "noticias relacionadas con la tecnología y la infancia" para los padres y profesores en más de 50 países.
- **NetAlert Limited** (<http://www.netalert.net.au>) – Organización comunitaria sin ánimo de lucro, creada por el gobierno australiano con el fin de ofrecer asesoría e información independientes acerca de la gestión del acceso al contenido en línea.
- **NetSmartzKids** (<http://www.netsmartzkids.org>) – NetSmartz es el recurso sobre la seguridad, que es interactivo e informativo, del National Center for Missing & Exploited Children (NCMEC) y del Boys & Girls Clubs of America (BGCA), para niños entre 5 y 17 años, padres, guardianes, profesores y autoridades, en el que se emplean actividades 3-D adaptadas para al público en cuestión, que sirven para enseñar a los niños a utilizar seguramente Internet.
- **Safe Kids Worldwide** (<http://www.safekids.org>) – Red mundial de organizaciones cuya misión es prevenir los accidentes, una de las principales causas de mortalidad de los menores de 14 años.
- **SafeKids.com** (<http://www.safekids.com>) – Recursos útiles para que las familias se sirvan de la tecnología y de Internet de una manera divertida, segura y productiva.
- **StaySafe.org** (<http://www.staysafe.org>) – Sitio informativo que pretende ayudar a los consumidores a entender los aspectos positivos de Internet, y a ocuparse de diversos aspectos relacionados con la seguridad en línea.
- **UNICEF** (<http://www.unicef.org>) – Organización mundial que aboga por los derechos de los niños, y que se dedica a proporcionar ayuda humanitaria y al desarrollo a largo plazo a niños y padres de los países en desarrollo.
- **WebSafe Crackerz** (<http://www.websafecrackerz.com>) – Juegos y rompecabezas interactivos que ayudan a los adolescentes, y ofrecen estrategias para hacer frente a diferentes situaciones en línea, tales como el correo electrónico indeseado (correo basura), la usurpación de claves y contraseñas, y las estafas.

I.2 Ejemplo de lista de contactos en caso de aumento de incidentes

En el cuadro I.1 se presenta un ejemplo de lista de contactos en Internet en caso de aumento de incidentes relacionados con la seguridad:

Cuadro I.1 – Ejemplo de lista de contactos en caso de aumento de incidentes

Organizaciones	Contacto
Cisco Systems Inc.	mailto:safetyandsecurity@cisco.com http://www.cisco.com/security
Forum of Incident Response and Security Teams (FIRST)	http://www.first.org/about/organization/teams/
Microsoft Corporation	mailto:avsubmit@submit.microsoft.com mailto:secure@microsoft.com
Telecom-ISAC Japan	https://www.telecom-isac.jp/contact/index.html

Bibliografía

- [b-UIT-T X.1051] Recomendación UIT-T X.1051 (2004), *Sistemas de gestión de seguridad de la información – Requisitos para telecomunicaciones (ISMS-T)*.
- [b-ISO/CEI 27001] ISO/CEI 27001:2005, *Information Technology – Security Techniques – Information Security Management Systems – Requirements*
<http://www.iso.org/iso/catalogue-detail?csnumber=42103>.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación