RECOMENDACIONES DE SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

27 de enero de 2011

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el **Centro Criptológico Nacional** puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. Introducción

El objeto de la presente guía es proporcionar una serie de recomendaciones de seguridad que permitan configurar de forma segura un equipo, mantenerlo protegido contra cualquier tipo de ataque externo y minimizar los posibles daños.

El concepto de seguridad de las TIC es mucho más amplio que la simple protección de los datos a nivel lógico. Para proporcionar una seguridad real se han de tener en cuenta múltiples factores, tanto internos como externos. En primer lugar, habrá que caracterizar el Sistema que va a manejar la información para poder identificar las amenazas y en este sentido se pueden encontrar:

- Sistemas aislados. Sistemas que no están conectados a ningún tipo de red.
- Sistemas interconectados. Hoy en día, casi cualquier ordenador pertenece a alguna red, enviando y recibiendo información del exterior casi constantemente.

Los objetivos de la Seguridad de las TIC se concretan en el mantenimiento de las características siguientes:

- Confidencialidad. Que la información sea revelada exclusivamente a los usuarios autorizados.
- Integridad. Que la información sea modificada sólo por personal autorizado. La integridad garantiza la exactitud de la información contra la alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.
- Disponibilidad. Que la información sea utilizable cuándo y cómo lo requieran los usuarios autorizados.

La seguridad absoluta, con una probabilidad del 100 %, es imposible de alcanzar ya que las medidas de seguridad a implementar deben ser proporcionales a los riesgos. Siempre hay que adoptar un compromiso entre el nivel de seguridad, los recursos disponibles y la funcionalidad deseada.

La implementación de seguridad es un compromiso entre costes y facilidad de uso frente a protección. Se deben planificar y tener en cuenta los pasos siguientes:

- Análisis de Riesgos. Estudiar los riesgos posibles y valorar las consecuencias de los mismos sobre los activos (información).
- Gestión de Riesgos. Valorar las diferentes medidas de protección y decidir la solución que más se adecue a la Organización (determinación del riesgo residual).
- Política de Seguridad. Adaptar la operativa habitual de la Organización a las nuevas medidas de seguridad.
- Mantenimiento. Observación continua de las medidas de seguridad, así como la adecuación de las mismas a la aparición de nuevas tecnologías.
- Planes de Contingencia. Determinación de las medidas a adoptar ante un incidente de seguridad.

La combinación de estas prácticas ayuda a proporcionar el nivel de protección **mínima** para mantener los datos a salvo.

2. Protección de Equipos

2.1. Seguridad en datos personales

2.1.1. *Copias de seguridad de los datos cruciales*

La realización de copias de seguridad implica llevar a cabo una copia de los datos en otro medio diferente del que se encuentren con el

fin de que estas copias adicionales puedan utilizarse para restaurar la información original después de una eventual pérdida de datos.

Las pérdidas de datos pueden deberse a robos, fallos en el Sistema, catástrofes naturales o simplemente a errores en el hardware del Sistema.

Existen muchos tipos diferentes de dispositivos empleados para el almacenamiento de datos, que son útiles para realizar copias de seguridad, con ventajas y desventajas a tener en cuenta a la hora de elegirlos.

Es recomendable verificar la integridad de las copias de seguridad con la debida frecuencia mediante la restauración real de los datos en una ubicación de prueba y así comprobar que están en perfecto estado de recuperación.

2.1.2. *Permisos*

La mayoría de los sistemas de archivos permiten asignar permisos o derechos de acceso a los mismos para determinados usuarios y grupos de usuarios. De esta manera, se puede restringir o permitir el acceso de un usuario a un archivo para concederle diferentes permisos.

En vez de conceder a todos los usuarios el acceso como "Administrador", es necesario crear una cuenta de usuario “**Invitado”**, si el ordenador va a ser usado, alguna vez, por otra persona distinta a la habitual. La creación de esta cuenta especial incorpora permisos muy limitados.

2.1.3. *Borrado seguro de datos*

Se puede pensar que un simple formateo del disco duro impediría que los datos almacenados en éste pudieran ser recuperados, pero resulta bastante sencillo obtener archivos que hayan sido borrados de un disco.

Algunos programas permiten deshacer el formateo de una determinada unidad e existen incluso métodos para recuperar los datos de los discos aunque estos hayan podido ser sobrescritos.

Si se quiere garantizar que no se distribuya información privada, se debe sobrescribir los

datos de forma que no sea posible recuperarlos de ningún modo.

Recomendación

Es necesario realizar diversas pasadas de escritura sobre cada uno de los sectores donde se almacena la información. Para simplificar la tarea lo más sencillo es utilizar algún programa especializado.

2.1.4. *Cifrado de datos*

Cifrar los datos significa convertir texto plano en texto ilegible, denominado texto cifrado, evitando que la información sea accedida por terceros no autorizados. Por lo general, la aplicación concreta del algoritmo de cifrado, se basa en la existencia de una clave: información secreta para realizar el proceso de transformación de los datos, que debe mantenerse en secreto.

Existen múltiples soluciones comerciales para cifrar los equipos informáticos que se pueden clasificar en tres tipos, atendiendo en qué nivel del sistema de archivos actúan:

- Cifrado de disco

  Es una tecnología que cifra el disco completo. El sistema operativo se encarga de descifrar la información cuando el usuario la solicita. Este sistema hace ilegible el disco duro si se intentara leer en otro equipo sin tener las claves de entrada.

- Cifrado de carpetas

  En este tipo de tecnología, el cifrado se realiza a nivel de carpeta. El sistema de cifrado se encargará de cifrar y descifrar la información cuando se utilice la carpeta protegida.

- Cifrado de documentos

  Esta es la tecnología más avanzada de las tres. El sistema se encarga de mostrar y permitir el acceso al documento solo a las personas autorizadas, haciendo ilegible el contenido a aquellas personas que no estén autorizadas.

2.1.5. *Impresión segura*

Los documentos y transacciones impresas son susceptibles de violaciones de la seguridad.

Por lo tanto, resulta fundamental emplear buenas prácticas para cumplir la normativa existente y que la información impresa no sea accesible por terceras personas no autorizadas.

2.1.6. *Sistemas de Alimentación Ininterrumpida (SAI)*

Un SAI es un equipo eléctrico encargado de alimentar y proteger cargas críticas, de tal manera que, aún faltando el suministro normal de red, es capaz de seguir alimentando a dicha carga durante un tiempo determinado.

Los parámetros más relevantes, que distinguen a un SAI de otro, son la potencia y la autonomía.

En general, para instalar un SAI debe tenerse en consideración lo siguiente:

- Nivel de seguridad deseado.
- Calidad del suministro eléctrico.
- Climatología
- Disponibilidad económica.

2.1.7. *Contraseñas*

Las contraseñas son el principal mecanismo de autenticación utilizado por las personas en su acceso a los Sistemas de información.

La seguridad que proporcionan las contraseñas depende, en gran medida, de su confidencialidad.

Características de una contraseña segura:

- No podrá ser asociada con facilidad a cualquier información relacionada con el usuario de la cuenta.
- Tendrá una longitud mínima de ocho caracteres.
- No utilizar la misma contraseña en dos Sistemas diferentes. Se debe tener contraseñas distintas en cada sitio. Si no
- se cumple esta regla y alguien la descubre, la contraseña podrá utilizarla múltiples veces en diferentes Sistemas.
- Combinar diferentes tipos de caracteres tipográficos: mayúsculas, minúsculas, números y caracteres especiales.
- Cambiar las contraseñas periódicamente.
- No compartir las cuentas y contraseñas con otros usuarios.
- No anotar las contraseñas en sitios de fácil acceso, ni almacenarlas en ficheros en el ordenador sin proteger.
- No utilizar la posibilidad de “Recordar Contraseña” que ofrecen algunos navegadores Web.

Existen programas que permiten almacenar todas las contraseñas con su nombre de usuario asociado en un sólo lugar, de forma que siempre estén disponibles y no haga falta recordarlas todas.

Habitualmente, estos programas disponen también de un generador de contraseñas seguras.

2.1.8. *Protección de datos personales*

Una de las obligaciones básicas establecidas por la LOPD[1] es la inscripción de los Ficheros

[1] Ley Orgánica de Protección de Datos Agencia Española de Protección de Datos https://www.agpd.es/

de datos de carácter personal en la Agencia Española de Protección de Datos.

2.2. Seguridad en dispositivos móviles

Es muy importante que los usuarios sean conscientes de la importancia de la seguridad en los aparatos móviles y los peligros que puede llevar consigo un mal uso.

Recomendaciones para trabajar en aéreas públicas

- Evitar trabajar con documentación sensible.
- No aceptar conexiones de dispositivos no conocidos para evitar transferencias de contenidos no deseados.
- Evitar conversaciones sobre información sensible.
- Evitar el uso de impresoras o faxes públicos, como los ubicados en hoteles. Si es imprescindible su empleo, es necesario asegurarse que se eliminan documentos temporales, pruebas de impresión o copias parciales.
- Ignorar y borrar SMS o MMS de origen desconocido que induzcan a descargas o accesos a sitios potencialmente peligrosos.
- Activar mediante PIN el acceso a la conectividad mediante Bluetooth.
- Configurar el dispositivo en modo oculto, para que no pueda ser descubierto por atacantes.

Directrices de seguridad específicas para los dispositivos portátiles

- Bloquear la tarjeta SIM en caso de pérdida.
- Emplear las diferentes opciones de bloqueo del dispositivo terminal.
- No descargar software de sitios poco fiables.
- Desactivar los dispositivos infrarrojos mientras no vaya a utilizarse.

2.3. Aplicaciones

La instalación de programas puede afectar al rendimiento y la seguridad del equipo. Debe mantenerse la integridad y siempre instalar software autorizado y proporcionado directamente por el fabricante.

Algunos aspectos a tener en cuenta a la hora de instalar programas son:

- Licencia y derechos de uso del programa: El uso de software ilegal además de generar riesgos de carácter penal, también puede generar problemas en la seguridad de la información. El software legal ofrece garantía y soporte.

- Certificación del programa para su compatibilidad con el sistema operativo y las demás aplicaciones.
- Instalación y mantenimiento de parches y actualizaciones de seguridad, sobre todo prestar atención a aquellas que son de carácter crítico.

2.4. Protección de máquina

2.4.1. *Software antivirus*

Los virus, así como los gusanos y los troyanos, son programas maliciosos que se ejecutan en su equipo. Entre las acciones que pueden provocar este tipo de código malicioso se encuentran: borrado o alteración de archivos, consumo de recursos del equipo, acceso no autorizado a archivos, infección de equipos remotos mediante correo electrónico… Existen herramientas de eliminación de software malicioso que comprueban infecciones por este tipo de código que ayudan a eliminarlas.

El propósito principal de las herramientas antivirus y antimalware es impedir el acceso de aplicaciones o programas maliciosos a nuestro ordenador, examinando el contenido de los archivos en busca de indicios de código malicioso.

Las funciones mínimas que se pueden esperar de una buena herramienta de antivirus y antimalware son las de filtrado entrante y saliente de contenidos maliciosos, protección en el correo electrónico, en la navegación y en las conexiones de todo tipo en redes corporativas o públicas. También deben analizar los ficheros presentes en discos externos y dispositivos USB permitiendo programar análisis exhaustivos cada cierto tiempo.

Recomendaciones

- Es necesario actualizar periódicamente los antivirus con las últimas definiciones para que el software pueda detectar los nuevos especímenes de virus.
- Pueden escogerse entre una gran variedad de antivirus, algunos de pago y otros gratuitos.
- Analizar con un antivirus todo lo que se descarga antes de ejecutarlo en el equipo.

2.4.2. *Actualizaciones de software*

Cualquier programa de ordenador necesita de actualizaciones periódicas para solucionar posibles problemas que hayan podido descubrirse u ofrecer una nueva funcionalidad. Estas actualizaciones son especialmente importantes en el sistema operativo.

Cada programa dispone de una manera particular de ser actualizado y es necesario instalar las actualizaciones tan pronto se

pongan a la disposición del público por parte de los fabricantes de software.

Una opción cómoda es permitir la opción de actualizaciones de seguridad de manera automática.

Además de mantener actualizado el sistema operativo es importante, también, actualizar el resto de programas que estén instalados en el ordenador.

2.4.3. *Firewall*

Un firewall es un programa encargado de analizar tanto el tráfico entrante como saliente de un equipo, con el fin de restringir la entrada de las posibles amenazas.

3. Navegación Internet

3.1. Seguridad en una red Wi-Fi

Si se trabaja con una red inalámbrica, para maximizar seguridad en la red Wi-Fi es necesario prestar atención a las siguientes recomendaciones.

3.1.1. *Asegurar el punto de acceso*

Todos los fabricantes establecen una contraseña por defecto de acceso a la administración del Punto de Acceso.

Al usar un fabricante la misma contraseña para todos sus equipos, es fácil o posible que el intruso la conozca, por lo tanto es recomendable cambiar la contraseña por defecto.

3.1.2. *SSID*

- Ocultar el identificador SSID al exterior es una buena medida para evitar las intrusiones.
- Es preferible escoger un nombre que resulte poco llamativo como puede ser "Desconectado", para tener menos posibilidades de que intenten entrar en nuestra red.
- El “broadcasting SSID” permite que los nuevos equipos que quieran conectarse a la red Wi-Fi identifiquen automáticamente los datos de la red inalámbrica, evitando así la tarea de configuración manual. Es recomendable desactivarlo, para ello será necesario introducir manualmente el SSID en la configuración de cada nuevo equipo que se quiera conectar.

3.1.3. *Datos transmitidos*

Sólo es recomendable utilizar cifrado WPA2 (Wi-Fi Protected Access).

3.1.4. *Restricciones de acceso*

Es necesario activar el filtrado de direcciones MAC de los dispositivos Wi-Fi.

Al activar el filtrado MAC, se permitirá sólo el acceso a los dispositivos que se conecten a la red con las direcciones MAC autorizadas.

3.2. Navegación segura

Algunas recomendaciones útiles:

- Acceder únicamente a sitios de confianza.

- Mantenga actualizado su navegador a la última versión disponible ofrecida por el fabricante.
- Descargar los programas desde los sitios oficiales para evitar suplantaciones maliciosas (Phishing).
- Configurar su navegador para evitar ventanas emergentes.
- Utilizar un usuario sin permisos de Administrador para navegar por Internet, es la mejor manera de evitar la instalación de programas y modificaciones en los valores de la configuración del sistema.
- Borrar las cookies, los ficheros temporales y el historial cuando utilice equipos ajenos para no dejar rastro de su navegación.

3.2.1. *DNI electrónico*

- La administración electrónica y la posibilidad de realizar operaciones y gestiones oficiales a través de Internet facilitan la operativa diaria en gestiones de diversa índole.
- Muchas administraciones públicas cuentan con accesos para el ciudadano que desea realizar operaciones con un DNI electrónico.
- El DNI electrónico[2] posee un microchip de seguridad que almacena unas claves de cifrado y firma digital, que permiten la identificación desde cualquier parte ante las administraciones.
- Contar con el DNI-e aporta un nivel adicional de seguridad en las operaciones.

3.3. Comercio electrónico

Internet es un medio ideal para comprar productos con diferentes ventajas asociadas, como la posibilidad de comprar en todas las partes del mundo y de una manera muy rentable y sin gastos de intermediarios, pero las compras en Internet pueden tener riesgos asociados que hay que tener en cuenta.

Recomendaciones

- HTTP seguro: Cuando se navega por páginas con información confidencial no interesa que esa información pueda ser leída por nadie, por lo que no debe utilizarse el protocolo HTTP habitual, sino el protocolo HTTP seguro, que permite, además de ocultar la información que se transmite, asegurar que la página a la que se conecta el navegador no ha sido suplantada por otra.
- Es buena idea disponer de cualquier otro medio de pago diferente al habitual, que

[2] Portal Oficial sobre el DNI electrónico http://www.dnielectronico.es/

permita controlar de forma estricta los límites de pago.

- Buscar referencias de los sitios Web donde se vayan a realizar los pagos.

4. Prevención y Protección

A primera vista, hay que tener en cuenta lo siguiente como buenas prácticas:

- Trabajar habitualmente en su Sistema como usuario sin privilegios, no como administrador.
- No ejecutar nunca programas de origen dudoso o desconocido.
- Utilizar software original.
- Si se emplea un paquete de software ofimático capaz de ejecutar macros, hay que asegurarse de que está desactivada la ejecución automática de éstas. Si no se pueden desactivar, emplear otro programa.

El riesgo de ser infectado por código malicioso será mayor allí donde haya una gran comunidad de usuarios y formas de trabajo que permita intercambio de información (dispositivos removibles) sin ningún tipo de control y restricción.

La protección contra código malicioso debe basarse, al menos, en la implementación de las siguientes estrategias:

- Instalación de software antivirus con actualizaciones regulares: productos de casas comerciales de confianza, que permitan una combinación de los siguientes métodos:
  - Escáner de acceso: permite examinar los archivos cuando son abiertos.
  - Escáner a demanda: análisis de virus que se llevarán a cabo en base a un calendario establecido.
  - Escáner de correos electrónicos: instalados en dispositivos de protección de perímetro o servidores de correo, los cuales deberían chequear los mensajes antes de ser tratados por la aplicación de correo.
  - Control de firmas: esta funcionalidad, a menudo incluida en los productos antivirus, permite detectar cambios no legítimos en el contenido de un archivo.
  - Métodos heurísticos: componente habitual en soluciones antivirus que busca firmas/comportamientos de virus modelo en archivos ejecutables.
- Implementación efectiva de control de configuración y gestión de software: se trata de asegurar que los sistemas operativos y aplicaciones son actualizadas de forma correcta tras la publicación de los parches preceptivos. Hay que considerar las siguientes reglas:
  - Todos los archivos ejecutables y plantillas de documentos “templates” compartidos deben estar colocados en un directorio de sólo lectura.
  - Cada usuario debe tener su propio directorio personal en la red con acceso lectura/escritura y restringido para

lectura para otros usuarios para prevenir previsibles diseminaciones de virus de la máquina local a la red.

– Los directorios compartidos por varios usuarios es un modo habitual de trabajo por lo que hay que prevenir la diseminación de posibles infecciones.

- Copias de respaldo: es fundamental realizar copias de respaldo de manera regular para asegurar la integridad del Sistema.
- Programas de formación y concienciación: esto es el factor más importante en cualquier política de prevención de infección por virus. Los usuarios deben ser conscientes de que la introducción de software no autorizado puede causar la infección del Sistema más protegido.

Los usuarios deben estar advertidos constantemente de la aplicación de las siguientes normas:

- Analizar y escanear, antes de su uso, cualquier información introducida o distribuida por dispositivos de almacenamiento removibles.
- Solamente los administradores del Sistema deberían estar autorizados para instalar software.
- Especial precaución con todos los adjuntos incluidos en los correos electrónicos.
- Proteger contra escritura, en la medida de lo posible, todos los dispositivos de almacenamiento removible.
- No ponerse nervioso en caso de infección y solicitar ayuda a los responsables de seguridad.

5. Reacción

Una vez que se ha detectado una infección, hay que seguir los siguientes pasos:

- Identificar y aislar los servidores, ordenadores y medios infectados.
- Desconectar físicamente de la red los elementos infectados en base al tipo y lugar donde se ha detectado el virus.
- Suspender cualquier intercambio de información entre el elemento infectado y el resto del Sistema.
- Rastrear y alertar a potenciales receptores de información de la presencia de máquinas infectadas.

6. Recuperación

La recuperación ante un ataque causado por un virus implica las siguientes acciones:

- Borrar y eliminar los virus del medio infectado.
- Recuperar el área afectada por la infección mediante la utilización de copias de respaldo. El alcance y escala de daño dependerá del tipo de virus.
- Vigilancia contra reinfecciones.
- Considerar el impacto de que el ataque aparezca en los medios de comunicación social.

7. La estrategia de seguridad

El diseñar una estrategia de seguridad depende en general de la actividad que se desarrolle, sin embargo, se pueden considerar los siguientes pasos:

- Crear una Política de seguridad.
- Realizar un análisis de riesgos.
- Aplicar las salvaguardas correspondientes.
- Concienciar a los usuarios

La Política de seguridad establece el estado en que se encuentra la información dentro de la Organización y debe contener un objetivo general, además hay que señalar la importancia de las tecnologías de la información para la Organización, el período de validez de la política, los recursos con que se cuenta y los objetivos específicos a cubrir.

Con el análisis de riesgos se consigue identificar los riesgos a los cuales está expuesta la información y cuáles son los impactos, las posibles amenazas y las vulnerabilidades que pueden ser explotadas por éstas.

Una vez que se establece la política de seguridad, determinando el riesgo residual que se está dispuesto a aceptar, se deben establecer las salvaguardas que den cumplimiento a la misma. La gestión de riesgos utiliza los resultados del análisis de riesgos para seleccionar e implantar las medidas de seguridad adecuadas para controlar los riesgos identificados y que se pueden dividir en las siguientes:

- Preventivas: (tienen como objeto reducir el riesgo)
  - Protección Física: guardias, control de acceso, protección hardware, ...
  - Medidas Técnicas: cortafuegos, detectores de intrusos, criptografía, ...
  - Medidas Procedimentales: cursos de mentalización, actualización de conocimientos, normas de acceso a la información, sanciones, ...
- Detectivas: (orientadas a la identificación del riesgo)
  - Protección Física: sistemas de vigilancia, detectores de movimiento, ...
  - Medidas Técnicas: control de acceso lógico, sesión de autenticación, ...
  - Medidas Procedimentales: monitorización de auditoría, ...
- Correctivas: (se orientan a impedir o reducir el impacto sobre los activos)
  - Protección Física: respaldo de fuente de alimentación (SAI), ...
  - Medidas Técnicas: programa antivirus, auditorías, respaldo de seguridad,...
  - Medidas Procedimentales: planes de contingencia, ...

La amenaza más seria para un Sistema de información son las personas, por consiguiente, la formación y sensibilización del personal es uno de los objetivos fundamentales que se persiguen con la implementación de un

programa de concienciación en seguridad. Los diferentes usuarios de los Sistemas deben asumir su responsabilidad en la protección de la confidencialidad, integridad y disponibilidad de los activos (información) de la Organización y comprender que esto no es sólo competencia de los especialistas en seguridad.

La seguridad debe considerarse como parte de la operativa habitual, no como un extraño añadido, es fundamental la incorporación de la seguridad a la actividad laboral.

El programa de mentalización y sensibilización debe perseguir dejar claro no sólo cómo proteger los Sistemas sino también porqué es importante su protección y cómo los usuarios se convierten en la primera barrera de seguridad para ellos. La implementación del programa ayuda a minimizar los costos ocasionados por los incidentes de seguridad dado que actúa directamente sobre uno de los eslabones más débiles en la cadena de seguridad, los usuarios.

Como colofón, se puede decir que no existe un Sistema que garantice al 100% la seguridad de la información que maneja debido a la inmensa cantidad de vulnerabilidades que presentan y lo que es más importante la imposibilidad de contar con los suficientes recursos para hacerlas frente, por tanto siempre hay que aceptar un riesgo, el conocido como riesgo residual.

Anexo I. Glosario de Términos y Abreviaturas

Término o abreviatura	Definición
BackUp	Copia de seguridad.
Bot	Realizan una amplia variedad de tareas automatizadas. Las tareas que los bots realizan son de la más amplia gama, desde enviar spam hasta eliminar sitios web de Internet como parte de un ataque coordinado de "negación de servicio". Muchas personas se refieren a los equipos víctima como "zombis".
Gusanos	Programa parecido a un virus, cuya principal característica es la capacidad de poder replicarse a si mismos
Malware	Malware o software de actividades ilegales es una categoría de código malicioso que incluye virus, gusanos y caballos de Troya. El malware también busca explotar en silencio las vulnerabilidades existentes en sistemas.
Pharming	El pharming redirige a sus víctimas al sitio web falso, incluso si escriben correctamente la dirección web de su banco o de otro servicio en línea en el navegador de Internet.
Phishing	El phishing o robo de identidad es básicamente un tipo de estafa en línea. Utilizan spam, sitios Web falsos, mensajes de correo electrónico, mensajes instantáneos con los que engañan a los usuarios para que divulguen información confidencial.
Spam	El spam es la versión electrónica del correo basura. Supone enviar mensajes no deseados a una gran cantidad de destinatarios y, por lo general, se trata de publicidad no solicitada.
Spyware	Programas espía que recopilan información.
Virus	Malware cuyo cometido es alterar el funcionamiento normal de un ordenador.
Vulnerabilidades en el Software	Debilidad en el software que podría ser explotada.

Anexo II. Referencias

Portal CCN-CERT – Capacidad de respuesta a Incidentes de Seguridad de la Información en las Administraciones Públicas https://www.ccn-cert.cni.es
CCN-STIC 401 – Glosario de términos https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-Glosario_y_abreviaturas/401/index.html
Series CCN-STIC – Guías de seguridad de sistemas TIC en la Administración Pública https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=188&lang=es
Amenazas informáticas a dispositivos móviles http://www.pandasecurity.com/spain/homeusers/security-info/types-malware/mobile-threats/
Guide to Microsoft .NET Framework Security . http://www.nsa.gov/ia/_files/app/oldFiles/I331-010R-2004.pdf
Symantec http://mx.norton.com/security_response/browsewebsafely.jsp
National Cyber Security Alliance http://www.staysafeonline.org/
Guía del US-CERT http://www.staysafeonline.org/
OnGuard Online http://www.onguardonline.gov/default.aspx