Fundamentos Tecnológicos para el Tratamiento y Análisis de Datos

Tema 8. Seguridad en los sistemas de información

Índice

Esquema

SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

- La navegación por la web está sujeta a numerosos riesgos, vulnerabilidades y peligros.
- La seguridad en los sistemas de información afecta tanto al usuario final como a los propios oferentes de servicio.
- Actualmente supone uno de los pilares básicos de la propia actividad de una empresa. Ninguna empresa es ajena a esta problemática.
- Básicamente dos son las vulnerabilidades fundamentales de cualquier sistema de información: el *software* malicioso y los robos de identidad.

SOFTWARE MALICIOSO

El *software* malicioso o *malware* es un tipo de software cuyo objetivo es infiltrarse en un equipo o sistema informático sin el consentimiento del usuario.

Robos de identidad

Tratan de suplantar la identidad del usuario para, una vez obtenida, tener acceso total a la red de comunicación. Destacan el *phishing*, *pharming*, *ransomware* o *keyloggers*.

- **Virus informático**. Son programas informáticos que se instalan e infiltran en los dispositivos informáticos de forma que la información pueda quedar expuesta.
- ***Spyware***. Es un programa que se instala en el ordenador para espiar toda la información existente en el dispositivo.
- **Gusanos informáticos**. Son similares a los virus informáticos, pero no necesitan de intervención humana.
- ***Troyanos***. Es un tipo de *software* que intenta crear puertas o entradas al sistema para que otros programas maliciosos puedan entrar.

HERRAMIENTAS PARA LA SEGURIDAD

Las empresas disponen de una amplio abanico de herramientas para proteger sus sistemas de información. Se dividen si están orientados a garantizar el acceso al usuario.

Pilares de la seguridad de la información

Tres son los grandes pilares de la seguridad de la información en la empresas: la **confidencialidad**, la **disponibilidad** y la **integridad de los datos**.

- **Autenticación biométrica.** Uso de rasgos humanos para autenticarse.
- **Certificados digitales.** Permite identificarse, con plena validez jurídica.
- ***Token.*** Dispositivo físico que garantiza el acceso autorizado o a impedir dicho acceso a usuarios no autorizados.
- ***Firewall.*** Protege a una computadora o una red de computadoras evitando las intrusiones de usuario con acceso no autorizados.
- **Antivirus.** Software que ayuda a proteger a nuestra computadora contra la mayoría de los virus, gusanos, troyanos y otros programas que puedan infectar nuestra PC.

8.1. Introducción y objetivos

Navegar por la red, ya sea visitando páginas web, mirando el correo electrónico o haciendo uso de las redes sociales más comunes, es algo muy habitual para cualquier usuario; sin embargo, estas actividades aparentemente tan inocentes llevan consigo un riesgo adherido.

Este riesgo puede llevar al robo de datos del usuario tales como cuentas corrientes, contraseñas, credenciales, números de tarjetas de crédito o cualquier dato financiero, o bien, que los propios equipos de dicho usuario sean atacados por un *software* malicioso, dejándolos vulnerables para que los *hackers* puedan introducirse y así, disponer de cualquier información almacenada en los distintos dispositivos.

Las empresas en la red, si son de un volumen muy grande, disponen de equipos de seguridad dedicados única y exclusivamente a tratar de impedir los problemas anteriormente mencionados, mientras que las más pequeñas deben de contratar estos servicios para proteger a los usuarios de todos estos riesgos.

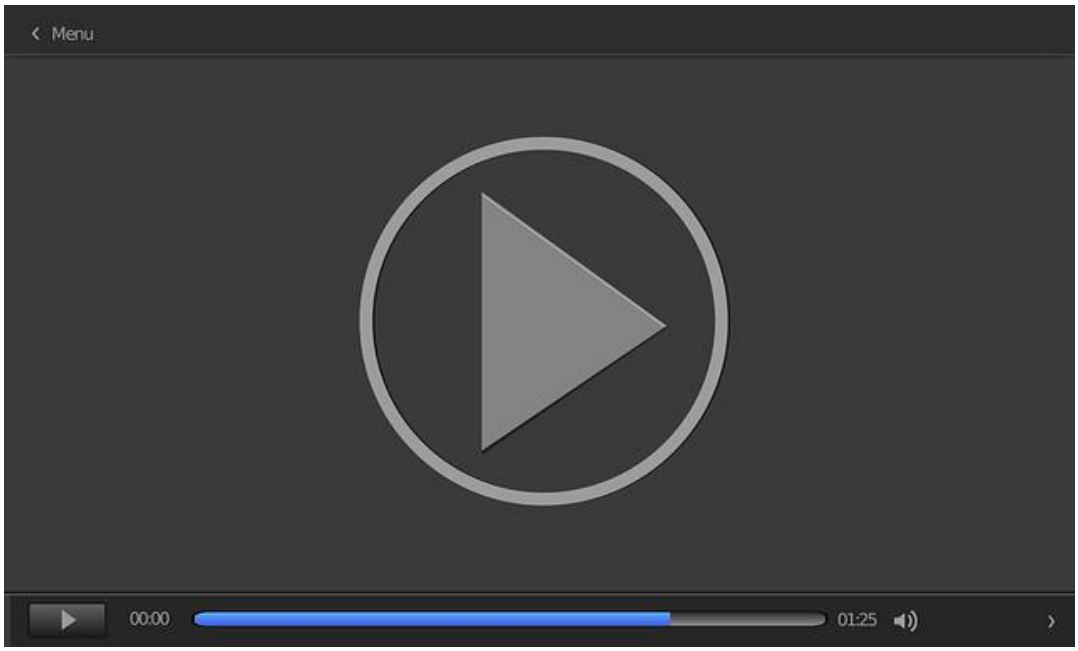
La seguridad en los sistemas de información no solo se refiere al individuo como usuario. Cuando este visita una web o revisa su correo electrónico, no solo él debe pensar en si los sistemas son seguros, sino también el oferente de los servicios anteriores debe garantizarla. Ningún usuario hará uso de un servicio en la red si tiene dudas acerca de la seguridad que proporciona ese servicio. Nadie se daría de alta en un servicio de correo electrónico si tuviera sospechas de que sus datos pueden verse comprometidos.

Por tanto, para cualquier empresa que proporcione servicios, la seguridad, entendiéndola como los procedimientos, medidas o medios para evitar el acceso a cualquier servicio sin autorización o permiso; debe ser uno de los pilares básicos de su actividad.

Ideas clave

En este contexto, con los conocimientos adquiridos en este tema el alumno será capaz de:

- Conocer los principios básicos de la seguridad en los sistemas de información.
- Saber cómo proteger la información de la empresa.
- Diferenciar entre los distintos tipos de herramientas que se utilizan en la seguridad de los sistemas de información.



Seguridad en los sistemas de información

Accede al vídeo:

https://unir.cloud.panopto.eu/Panopto/Pages/Embed.aspx?id=4417a03d-fd30-4e6e-b9f4-b16c00959e0b

8.2. Seguridad en los sistemas de información

La seguridad en los sistemas de información es muy vulnerable porque existen muchos elementos que se interconectan entre sí a través de las redes de comunicaciones. En este sentido, los accesos fraudulentos o sin autorización pueden venir originados desde diferentes puntos de acceso a la red, ya sea desde las líneas de comunicaciones, como los servidores, o desde el propio punto de acceso del usuario- cliente, entre otras vías.

Pero ¿cuáles son las **vulnerabilidades** que nos podemos encontrar en la red?

- En primer lugar, las **redes públicas grandes** (como el propio Internet), por definición, son mucho más vulnerables que las privadas o que las redes más reducidas, simplemente porque están abiertas frente a las otras. Además, el acceso a Internet es vía módem o ADSL principalmente. Este tipo de acceso presenta muchos peligros y vulnerabilidades y es muy susceptible a la piratería informática, ya que usan direcciones de Internet fijas, por lo que son objetivos muy identificados por parte de los *hackers*. Recordemos que el acceso no solo es de datos sino también de voz, este último es aún más vulnerable.

- Por otro lado, el aumento cada vez más mayor del uso del **correo electrónico o mensajería instantánea**, junto a los archivos adjuntos que este tipo de comunicación permite y donde pueden incluirse datos privados, comerciales o confidenciales ha hecho que este tipo de comunicación sea uno de los objetivos principales de los *hackers*.

- Finalmente, no debemos olvidarnos de las **redes P2P** para compartir datos, que son muy utilizados para transmitir *software* malicioso o exponer información privada.

Software malicioso

Podemos decir que existen dos tipos de riesgos fundamentales para cualquier

sistema de información: el *software* malicioso y los robos de identidad.

Software malicioso o malware

El *software* malicioso o *malware* es un tipo de *software* con el objetivo de infiltrarse en un equipo o sistema informático sin el consentimiento del usuario. Existen varios tipos como los virus informáticos, gusanos, caballos de troya o troyanos, *spyware*, *adware*, etc.

- Los **virus** no son más que programas informáticos (es necesario que el usuario ejecute el archivo donde se encuentre) que se instalan e infiltran en los dispositivos de forma oculta y se propaga por todo el *software*, haciendo que la información pueda quedar expuesta, disminuya el ancho de banda, ralentiza el funcionamiento normal del computador, pudiendo provocar pérdidas de información y daños irreparables.

- Los **gusanos informáticos** son similares a los virus, pero no necesitan de intervención humana, son bastantes difíciles de detectar y se multiplican con mucha facilidad. Suelen ser muy utilizados para el envío de correos desconocidos (*spam*) de forma masiva.

- El ***spyware*** es un programa que se instala en el computador para espiar toda la información existente en el dispositivo.

- Finalmente, los **troyanos** no son más que un determinado tipo de *software* que intenta crear puertas o entradas al sistema para que otros programas maliciosos puedan entrar. Recordemos que la mayor parte del *software* malicioso viene oculto en archivos aparentemente no peligrosos.

Robo de identidad

Finalmente, debemos de hablar de los robos de identidad, destacando, entre otros, el *phishing*, *pharming*, *ransomware* o *keyloggers*. Estos riesgos, como su nombre indica, tratan de suplantar la identidad del usuario para tener acceso total a la red de

comunicación.

- El más común de todos es el ***phishing***. Generalmente se ejecuta a través de un canal de comunicación, principalmente mediante correo electrónico, pidiendo al usuario que releve información personal (contraseñas, número de tarjeta de crédito, cuentas bancarias, etc.) proporcionando un enlace donde incorporar dicha información.

- El ***pharming*** redirige a los usuarios a sitios web falsos (simulando una página web legal) para que, al igual que el *phising*, el usuario introduzca sus datos que permitan luego suplantar su identidad en el sitio web real. Es importante señalar que este *software* muchas veces pasa totalmente inadvertido para el propio usuario, ya que el programa lo redirige hacia un sitio web falso que es prácticamente idéntico al verdadero.

- El ***ransomware*** es un tipo de ataque donde la víctima descarga un código malicioso que encripta el disco duro de un dispositivo impidiendo el acceso a este, el *hacker* pedirá un pago para desbloquearlo.

- Un *keylogger* o «capturador de teclas» es un *software* o *hardware* que guarda las pulsaciones realizadas en el teclado de un equipo infectado, capturando así la información escrita con el teclado. Estas pulsaciones son guardadas y luego enviadas al equipo del atacante.

Seguridad inalámbrica

Pasemos ahora a mostrar los **problemas derivados** de la seguridad inalámbrica. Actualmente el uso de computadores portátiles o *smartphones* es muy popular entre la población y el acceso a las redes (principalmente a Internet) se hace mayoritariamente a través de redes inalámbricas; ya sea en tu propia casa como en un hotel, aeropuerto o centro comercial.

Este tipo de redes, como el *bluetooth* o el wifi, son muy sensibles a accesos no

autorizados y, generalmente, no están abiertas y requieren una contraseña. En el caso del wifi, a finales del siglo pasado, se desarrolló el protocolo de privacidad equivalente al cableado (WEP por sus siglas en inglés), que prácticamente no se utiliza, ya que resulta muy fácil explotar su vulnerabilidad. Todavía vigente, este recurso fue abandonado en 2004 por la Alianza Wi-Fi.

Un año antes, se desarrolló el protocolo WPA (protocolo *Wi-Fi Protected Access*) que, al igual que el anterior, resulta ser muy vulnerable. Casi al mismo tiempo, se lanzó una segunda versión del protocolo WPA, el WPA2. Este protocolo es mucho más eficiente y seguro que los anteriores, pero sigue presentando muchas vulnerabilidades. Esta información es importante, ya que pone de manifiesto que:

Las **redes wifi** son una de las vulnerabilidades más importantes para cualquier sistema de información.

8.3. Seguridad de la información de la empresa

Como ya hemos advertido anteriormente, toda la información que posee una empresa es susceptible de ser robada o ser víctima de fraudes informáticos. Prácticamente, la totalidad de la empresa tiene sus datos (contables, financieros, recursos humanos, etc.) en un dispositivo o incluso en una red informática, y, casi seguro, esas redes cuentan con conexión a Internet.

Todo esto puede suponer un grave riesgo para la seguridad de cualquier empresa, ya que existe la posibilidad de que haya fugas o pérdidas de información, ya sea de mala fe por parte de *hackers* o empresas dedicadas al hurto o fraudes informáticos. No nos olvidemos que puede existir la posibilidad de que, sin una buena seguridad, la información de una empresa pueda estar al alcance de cualquiera.

Es por esto que los sistemas de gestión de seguridad de la información resultan vitales para la prevención de los problemas mencionados. Muchas empresas consideran un gasto este tipo de actuaciones, pero debería de calificarse como una **inversión**, ya que mantener la seguridad de la información de nuestra empresa a salvo puede suponer una eliminación de graves problemas con vistas al futuro.

Son tres **los grandes pilares de la seguridad de la información** en las empresas, la confidencialidad, disponibilidad e integridad de los datos.

- La **confidencialidad** se basa en garantizar el acceso a la información solo a los usuarios autorizados, impidiendo accesos fraudulentos o no autorizados.
- La **disponibilidad**, como su propio nombre indica, certifica que el acceso a la información se realiza de manera ágil y segura desde cualquier dispositivo.

Ideas clave

- La **integridad de los datos** garantiza que los datos son reales y correctos, es decir, no han sido modificados, manipulados o alterados, manteniendo la información como fue generada

Confidencialidad, disponibilidad e integridad de los datos son los aspectos básicos de la seguridad de la información en las empresas. Cualesquiera que sean los riesgos para la seguridad de la información en la empresa, siempre están orientados hacia estos tres pilares: desde el uso de dispositivos de almacenamiento móviles (disco duros portátiles, memorias USB) por parte de los empleados de la empresa, que hace que la información se traslade de un equipo a otro y, por tanto, maximizando el riesgo de entrada de *software* malicioso, pasando por la mala gestión existente en el uso de contraseñas y de permisos, que hace que un gran número de personas tengan acceso a gran parte de la información de la empresa, sin ningún control exhaustivo.

No podemos olvidarnos de que en cualquier empresa el **uso del correo electrónico** es vital para su funcionamiento. Por un lado, el riesgo de sufrir ataques informáticos a través de estos mensajes es muy grande, y, por otro, el envío masivo de correos puede poner al descubierto las identidades de los usuarios, no respetando la confidencialidad; algo tan simple como cerrar sesión después de cada jornada resulta una reducción del riesgo muy importante para la seguridad de la empresa.

Finalmente, numerosas empresas por diversas razones se sirven de ***software* pirata** (no oficial). Este tipo de *software* es una clara amenaza para la seguridad, ya que generalmente son de origen desconocido y la mayor parte de las veces son «ofertadas» de forma gratuita en la red con fines delictivos (inclusión de gusanos, troyanos, etc.).

Los riesgos son numerosos, pero, en principio, fácilmente subsanables siguiendo una serie de indicaciones:

Ideas clave

- Empezar con algo tan simple como que los propios empleados y usuarios sean conscientes de la necesidad de garantizar la seguridad en la empresa, no subestimando los riesgos existentes.
- Utilizar *software* original (y sus posteriores actualizaciones) que garantice un uso seguro de los archivos y el *software*; así como una buena gestión de contraseñas y permisos para evitar el acceso a la información de personas no autorizadas.
- La asignación de contraseñas y permisos individuales o el uso de la firma digital pueden ser buenas medidas, así como, la instalación de programas antivirus o evitar el correo no deseado (spam) o realizar copias de seguridad de forma periódica.

Todos los dispositivos informáticos de una empresa deben protegerse frente a amenazas que puedan resultar del uso de discos duros y USB, conexiones a redes wifi externas, *spam*, descargas de archivos de origen desconocido, etc.

8.4. Tecnologías y herramientas para proteger los sistemas de información

Las empresas disponen de un amplio abanico de herramientas para proteger sus sistemas de información, instrumentos para administrar, autentificar y proteger la identidad del usuario y, así, evitar el acceso no autorizado al sistema junto con la necesidad de asegurar el funcionamiento óptimo de su sistema.

Como ya hemos dicho, el primer paso versa sobre cómo obtener el acceso a un sistema. Para ello es necesario que el usuario tenga autorización, esté identificado y autentificado.

Autentificación

La autentificación es la capacidad de demostrar que un usuario o una aplicación o programa es realmente quien asegura ser. Durante mucho tiempo, la forma más usual ha sido mediante el uso de contraseñas o códigos tipo PIN que, obviamente, solo son conocidas por los usuarios autorizados. El problema de estas es que son susceptibles de ser olvidadas, sean simples y fáciles de adivinar o simplemente sean compartidas por varios usuarios.

Además, al ser combinaciones alfanuméricas son relativamente sencillas de obtener mediante procesos tales como el método de fuerza bruta, que consiste simplemente en ir probando todas las combinaciones posibles. Este método, existente desde los inicios, ahora es muy fácil de utilizar debido al aumento cuasiexponencial del rendimiento y la capacidad de cálculo de las computadoras.

Sin duda, en los últimos años, este sistema básico de autentificación ha sido superado por nuevas tecnologías o procedimientos que explicamos a continuación:

Autentificación biométrica

Se trata de usar partes de los rasgos humanos tales como una huella digital, un escaneo del ojo, retina o iris o la forma de la cara entre otras para autentificarse. En principio, presenta la gran ventaja de que es propio de cada usuario, muy fácil de usar y no es transferible, por lo que se reduce en gran medida la posibilidad de robo de identidad.

Actualmente la mayor parte de los *smartphones* y un gran número de computadores portátiles ya llevan incorporado algún tipo de autentificación biométrica, combinándolo muchas veces con las propias contraseñas, aunque el uso por parte de los usuarios aún es reducido.

Certificados digitales

Es un medio que permite identificarnos electrónicamente y, muy importante, con plena **validez jurídica**. Aunque existen varios tipos de certificados digitales, el más usado por la mayoría de los usuarios es el certificado de persona física. Con este, el usuario garantiza la identificación y la autentificación. El DNI electrónico o el certificado digital expedido por la FNMT (Fábrica Nacional de Moneda y Timbre) son dos buenos ejemplos.

Token

Es un aparato electrónico que se le da a un usuario autorizado de un servicio. Los *tokens* se usan para almacenar claves criptográficas, códigos PIN, contraseñas, firmas digitales o incluso datos biométricos, como las huellas digitales.

Mensajería bidireccional

Bien mediante correo electrónico, donde el usuario recibe a través de este un correo con el acceso a la aplicación o herramienta; o bien, por SMS, recibiendo un código para dicho acceso.

Herramientas de protección

Aparte del proceso de identificación y autentificación, los propios sistemas de información deben de protegerse de ataques. Es por ello que protecciones contra el acceso no autorizado o de infección *malware* han ido desarrollándose a lo largo de los años.

Los siguientes elementos son fundamentales para la seguridad informática:

Firewall o cortafuegos

Principalmente es un sistema que permite proteger a un computador o una red de computadores, evitando las intrusiones de usuarios con acceso no autorizado. Filtra el tráfico de red tanto entrante como saliente.

Podemos definirlo también como una combinación de programas (*software*) o equipos (*hardware*) que actúa como intermediario entre la red local (o la computadora local) y una o varias redes externas, permitiendo solo el tráfico que esté en la lista permitido.

Antivirus

Es un programa (*software*) que ayuda a proteger a nuestra computadora contra la mayoría de los virus, gusanos, troyanos y otros programas que puedan infectarla. La finalidad de estos programas es la de detectar y, posteriormente, eliminar los procesos antes mencionados. El principal hándicap de este tipo de programas es que solo son efectivos para procesos ya conocidos, por lo que es necesario una constante actualización.

Antispyware

Existen programas (*software*) que se instalan de forma oculta y malintencionada en un computador con el objetivo de espiar y enviar cualquier tipo de información (datos de la empresa, cuentas bancarias, contraseñas, etc.) al receptor del programa. Por todo ello, muchas veces se necesitan programas informáticos que son utilizados para

combatir o proteger de programas espías tales como *spyware, adware o keyloggers*. Al igual que el anterior, requiere de actualizaciones periódicas para un correcto y efectivo funcionamiento.

Antispam

En multitud de ocasiones la dirección de la cuenta de correo electrónico personal o de la empresa se puede encontrar en la red o, simplemente, haberla transmitido a cualquier persona. Por tanto, es posible que este correo electrónico reciba correos de origen desconocidos (*spam*) con la finalidad de introducir un virus a los equipos informáticos una vez abiertos.

Se calcula que alrededor del 80 % de los correos que circulan por la red son *spam*. Por ello, es prioritario tener un s*oftware antispam*, con el objetivo de minimizar dichos riesgos.

No se debe minimizar los retos a los que se enfrenta la empresa en relación a la seguridad de su información.

Oficina de seguridad del internauta (OSI)

INCIBE. Página oficial web. https://www.osi.es/es

Página web oficial de la Oficina de Seguridad del Internauta (OSI), adscrita al INCIBE (https://www.incibe.es/) y que proporciona al ciudadano la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet.

Su objetivo es reforzar la confianza en el ámbito digital a través de la formación en materia de ciberseguridad. En la OSI se trabaja para ayudar a los usuarios a adoptar buenos hábitos en seguridad, a hacerles conscientes de su propia responsabilidad en relación con la ciberseguridad y a contribuir a minimizar el número y la gravedad de incidencias de seguridad.

Asociación española para el fomento de la seguridad de la información

Recuperado de https://www.ismsforum.es/index.php

ISMS Forum Spain es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la seguridad de la información en España y actuar en beneficio de toda la comunidad implicada en el sector.

Creada con una vocación plural y abierta, se configura como un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales; donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de seguridad de la información. Toda su actividad se desarrolla con base en los valores de transparencia, independencia, objetividad y neutralidad.

Test

1. La seguridad de las empresas es un:

A. Gasto.

B. Inversión.

C. Ambos (A y B).

D. Ninguna de las anteriores.

2. La seguridad de la empresa solo supone un problema desde el punto de vista de los *hackers* u organizaciones delictivas:

A. Falso.

B. A veces son los propios clientes los que ven información que no deben.

C. No es solo un riesgo de cara a organizaciones delictivas.

D. Todas las anteriores.

3. La seguridad de la empresa es necesaria para:

A. El usuario final.

B. El gerente de la empresa.

C. Los trabajadores de la empresa.

D. Todas las anteriores.

4. Si recibimos un correo por parte de nuestra entidad bancaria solicitándonos nuestros datos debemos:

A. Llamar al banco para confirmar el correo.

B. Pasar el antivirus, *antispyware* o cualquier *software* que garantice que el correo es correcto.

C. Contestar incluyendo los datos solicitados.

D. Ninguna de las anteriores.

5. Conectarnos a una red wifi de acceso público y gratuito supone un riesgo:

   A. Depende del origen de la red.

   B. No.

   C. A veces.

   D. Sí.

6. La existencia de un virus en el computador supone:

   A. Un riesgo para la empresa.

   B. El computador va a tener un peor rendimiento.

   C. Puede llegar a inutilizar el computador y la pérdida de toda la información.

   D. Todas las anteriores.

7. Para proteger nuestro sistema debemos:

   A. Encriptar los datos.

   B. Crear copias de seguridad.

   C. Actualización periódica del software original y de contraseñas.

   D. Todas las anteriores.

8. La autentificación requiere de:

   A. Una contraseña.

   B. Un código PIN.

   C. Certificado digital.

   D. Todas las anteriores.

9. Un cortafuegos o *firewall* puede ser:

A. Un *software*.

B. Un *hardware*.

C. Ambos.

D. Ninguna de las anteriores.

10. El *spam* es:

A. Envío masivo de correos electrónicos con fines comerciales.

B. Envío de correos electrónicos con fines delictivos.

C. Pueden ser correos electrónicos, sms o mensajes en blogs, foros o páginas webs.

D. Todas las anteriores.