SEGURIDAD INFORMÁTICA

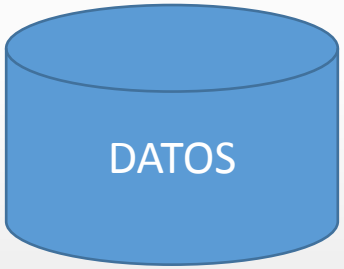
SEGURIDAD INFORMÁTICA

Se denomina seguridad informática al conjunto de acciones, herramientas y dispositivos cuyo objetivo es dotar a un sistema informático de:

- **Confidencialidad**: los datos solo son accesibles por las personas autorizadas.
- **Integridad**: los datos no han sido alterados por personas no autorizadas.
- **Autenticación**: verifica que un usuario es quien dice ser.
- **Disponibilidad**: garantiza a los usuarios autorizado el acceso a la información y a los recursos.
- **No repudio**: el receptor puede probar que el mensaje fue enviado por el presunto emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto receptor.

SOFTWARE - HARDWARE - DATOS

Hay tres elementos que hay que proteger en un sistema informático.



Reinstalable

Backup

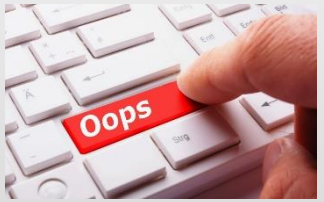
Reposición

NIVELES DE SEGURIDAD

- **Seguridad física**: conjunto de medidas para controlar el acceso físico a un elemento (puertas, cerraduras, rejas, paredes...) evitando el acceso no autorizado y su protección frente a fallos o desastres (incendios, inundaciones, terremotos, fallos de energía...).

- **Seguridad lógica**: medidas para controlar el acceso y manipulación de la información por terceras partes. Las contraseñas, cifrados, códigos, herramientas de seguridad (antivirus, cortafuegos...) son parte de la seguridad lógica.

- **Seguridad humana**: es la responsabilidad que el propio usuario toma sobre la información y las medidas y protocolos de conducta que lleva a cabo para gestionarla adecuadamente - *elección de contraseñas seguras, no divulgación de claves, el uso de herramientas de seguridad*-.



RIESGOS EN UN SISTEMA INFORMÁTICO

Usuarios: la causa del mayor problema ligado a la seguridad de un sistema informático son los propios usuarios (porque no les importa, no se dan cuenta o a propósito). Son los usuarios los que borran archivos, aceptan correos, eliminan programas, etc.

Intrusos: personas que consiguen acceder a los datos o programas a los que no tiene acceso permitido (crackers).

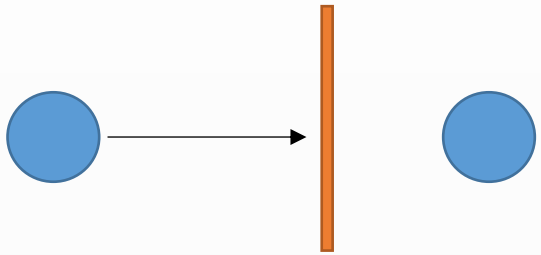
Siniestros: averías, accidentes, robo, incendio, inundación... una mala manipulación o una malintención derivan en la pérdida del material o de los datos.

Software malicioso (malware): software creado para instalarse en un ordenador ajeno sin el conocimiento del usuario para perjudicar o hacer un uso ilícito de los recursos del sistema.

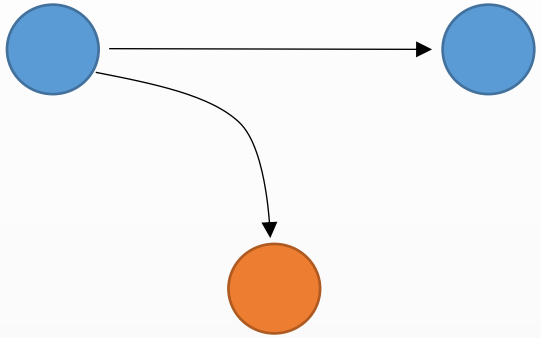
Vulnerabilidades: fallos de seguridad en el software que pueden provocar que nuestros sistemas informáticos puedan funcionar de manera diferente para lo que estaban pensados, afectando su seguridad, pudiendo provocar la pérdida y robo de información sensible.

https://www.cybermap.kaspersky.com/es

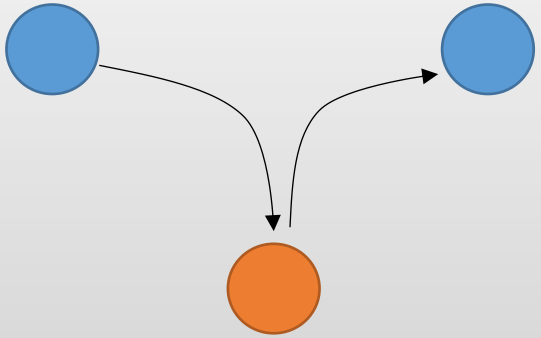
TIPOS DE ATAQUES



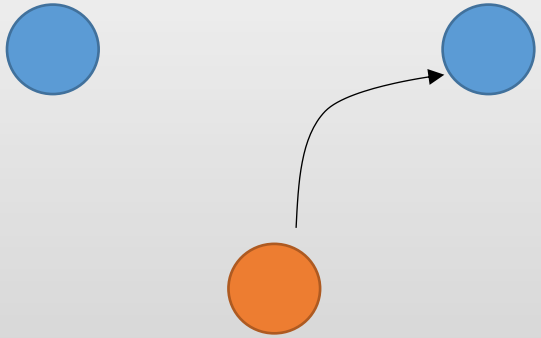
INTERRUPCIÓN



INTERCEPTACIÓN



MODIFICACIÓN



FABRICACIÓN

TÉCNICAS DE SEGURIDAD

Técnicas de seguridad activa: tienen como objetivo proteger y evitar posibles daños en los sistemas informáticos:

- Empleo de contraseñas adecuadas, que no se puedan deducir de datos personales, con una longitud apropiada, mezclando letras, números y símbolos, renovándolas periódicamente.

- Encriptación de datos consiste en convertir, mediante un algoritmo complejo, la información en algo ilegible, de manera que sólo el proceso inverso (con ayuda de una clave) puede devolver al archivo su forma original.

- Uso de software de seguridad informática como cortafuegos, antispyware, antivirus, llaves para protección de software, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

Técnicas de seguridad pasiva: su fin es minimizar los efectos o desastres causados:

- Decidir la ubicación y protección física adecuada de los equipos para proteger el hardware de los posibles desastres naturales, de incendios, inundaciones, robos, accesos indebidos y otra serie de amenazas. Se trata de aplicar barreras físicas y procedimientos de control de acceso para mantener la seguridad.

- Uso del hardware adecuado contra accidentes y averías, como por ejemplo un SAI (sistema de alimentación ininterrumpida)

- Realización de copias de seguridad de los datos y del sistema operativo. Para esto existe software libre como: Cobian Backup o Clonezilla, para Windows, Keep KDE para Linux.

Algoritmo C++ muestra las posibles combinaciones de 4 caracteres

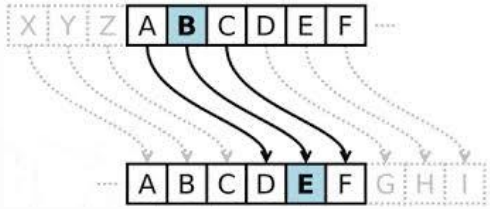
```
//string11.cpp
#include <iostream>
#include <stdlib.h>
#include <string>
using namespace std ;
//Combinaciones de 4 letras del alfabeto. 26^4= 456.976 combinaciones
int main()
{
        string alfabeto("abcdefghijklmnopqrstuvwxyz");
        int i,j,k,l;

        for (int i=0; i<26; i++)
                for (int j=0; j<26; j++)
                        for (int k=0; k<26; k++)
                                for (int l=0; l<26; l++)
                                        cout<<alfabeto[i]<<alfabeto[j]<<alfabeto[k]<<alfabeto[l]<<" ";
return 0;
}
```

Proccess exited after 77,4 seconds

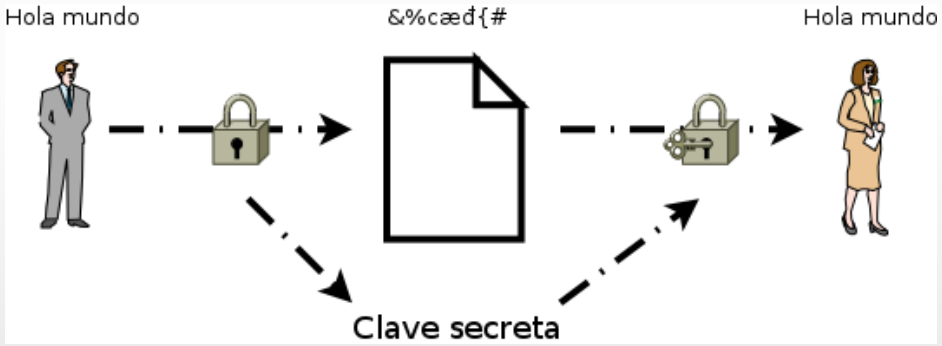
La ***Criptografía*** se ocupa del diseño de procedimientos para cifrar , es decir, para “enmascarar” una determinada información confidencial.

El ***Criptoanálisis***, se ocupa de romper esos procedimientos de cifrado para así recuperar la información original. Siempre se han desarrollado de forma paralela , pues cualquier método de cifrado tiene emparejado su Criptoanálisis correspondiente.

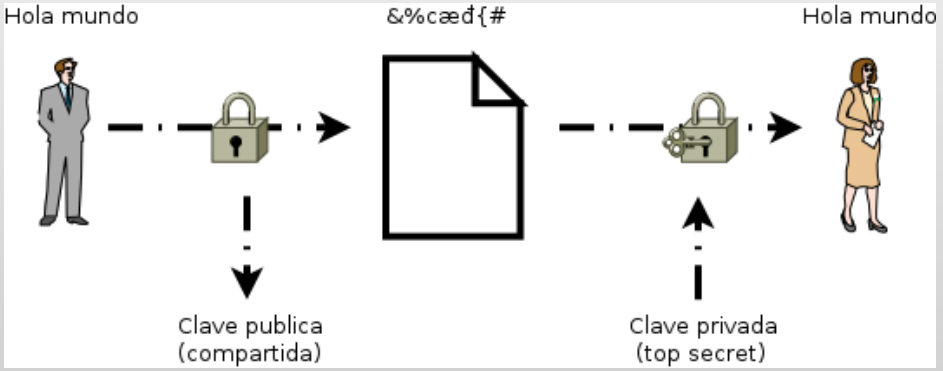
CIFRADO CLÁSICO



CIFRADO SIMÉTRICO



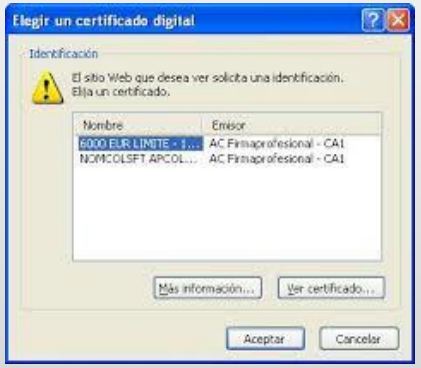
CIFRADO ASIMÉTRICO



Firma electrónica: Se trata del “conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medios de identificación del firmante”, según la Ley 59/2003. Este es por tanto un concepto jurídico y un método de identificación, equivalente o análogo a la firma manuscrita, que se sirve de diversos soportes electrónicos distintos, como un lápiz electrónico o una firma digital. Realizar una firma electrónica quiere decir que una persona física verifica una acción o procedimiento mediante un medio electrónico, dejando un registro de la fecha y hora de la misma. Este concepto es más genérico, amplio e indefinido desde el punto de vista electrónico que la firma digital.

La firma digital Es un mecanismo criptográfico de clave asimétrica o de doble clave que permite al destinatario de un mensaje firmado digitalmente comprobar la entidad que originó el mensaje y confirmar que este no ha sido modificado desde que fue firmado por el emisario.

Un Certificado Electrónico es un conjunto de datos que permiten la identificación del titular del Certificado, intercambiar información con otras personas y entidades de manera segura, y firmar electrónicamente los datos que se envían de tal forma que se pueda comprobar su integridad y procedencia.

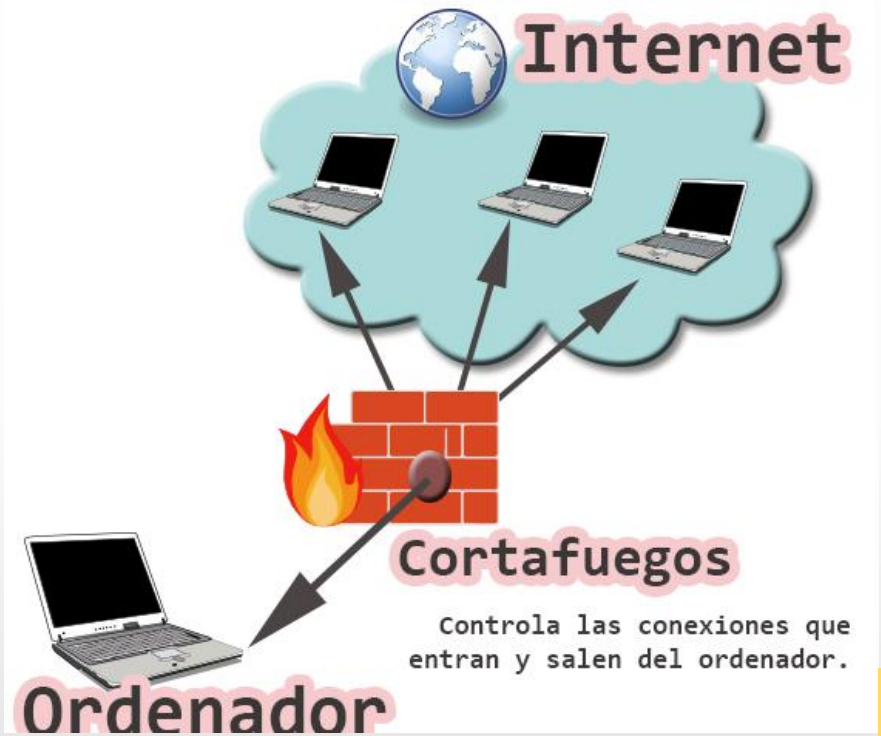


http://firmaelectronica.gob.es/Home/Ciudadanos/DNI-Electronico.html

ANTIVIRUS

Un **antivirus** es un programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.

CORTAFUEGOS O FIREWALL



Personales: Se instalan en el equipo

Profesionales: Pueden ser servidores con un software específico o hardware diseñado para este fin

Funciones:

1. Denegar todo el tráfico y añadir reglas de lo permitido.

2. Permitir todo y añadir reglas de prohibición

MODOS DE INFECCIÓN , TRANSMISIÓN Y PREVENCIÓN

Medios	Modos	Prevención
Internet	Inyección SQL, Correo, web, FTP, downloads, P2P Chat, Ingeniería social, …	Antivirus, Antispyware, Firewall, Configuración navegador …
Redes	Acceso malware	Antivirus, Antispyware, Firewall, Configuración navegador …
Unidades Extraíbles	Infectadas	Deshabilitar el autoarranque
Vulnerabilidad	Del Software	Actualizar Software

EFECTOS Y SÍNTOMAS DE INFECCIÓN

Es difícil adivinar a simple vista si un ordenador está siendo víctima de una amenaza. La certeza sólo se consigue usando un buen paquete integrado de seguridad correctamente actualizado. Sin embargo, hay ciertos síntomas que delatan la posible presencia de virus u otras amenazas en el ordenador (aunque también pueden deberse a otros problemas ajenos a los virus):

- Problemas generales del sistema
- Problemas en el arranque.
- Lentitud repentina.
- Constantes bloqueos con operaciones normales.
- Apagado y reinicio repentino del ordenador.
- Mal funcionamiento del disco duro.
- Disminución de capacidad de la memoria o del disco duro.
- La bandeja del CD-ROM se abre y se cierra automáticamente.
- El teclado y el ratón no funcionan correctamente o lo hacen al azar
- Problemas con archivos y programas
- Desaparición de ficheros, carpetas y programas.
- Alteración inesperada en las propiedades de un fichero (nombre, tamaño, fecha de creación, atributos...).
- Imposibilidad de acceder o guardar el contenido del archivo.
- Aparición de archivos duplicados con extensiones EXE y COM.
- Cierre repentino de un programa.
- Desaparecen ventanas y aparecen otras nuevas.
- Imposibilidad de ejecutar algunos programas.
- Avisos o mensajes
- Aparición en pantalla de avisos o mensajes de texto inesperados o publicitarios.
- Mensajes de error al realizar operaciones sencillas en condiciones normales.

¿DÓNDE SE ESCONDEN?

- Las páginas Web están escritas en un determinado lenguaje y pueden contener elementos (**Applets** Java y controles **ActiveX**) que permiten a los virus esconderse en ellos. Al visitar la página, se produce la infección.

- Los mensajes de correo electrónico pueden contener ficheros **adjuntos** infectados o incluso infectar con su simple lectura y apertura.

- Los virus y las amenazas se colocan y quedan **residentes** en la memoria principal del ordenador (RAM), esperando a que ocurra algo que les permite entrar en acción.

- El sector de arranque es un área especial de un disco, que almacena información sobre sus características y su contenido. Los virus, concretamente los de **boot**, se alojan en ella para infectar el ordenador.

- Los ficheros con **macros** son pequeños programas que ayudan a realizar ciertas tareas y están incorporados dentro de documentos Word (ficheros con extensión DOC), hojas de cálculo Excel (extensión XLS) o presentaciones PowerPoint (extensión PPT o PPS) y en ellos se pueden alojar también los virus.

CLASIFICACIÓN DEL MALWARE SEGÚN SU MODO DE PROPAGACIÓN

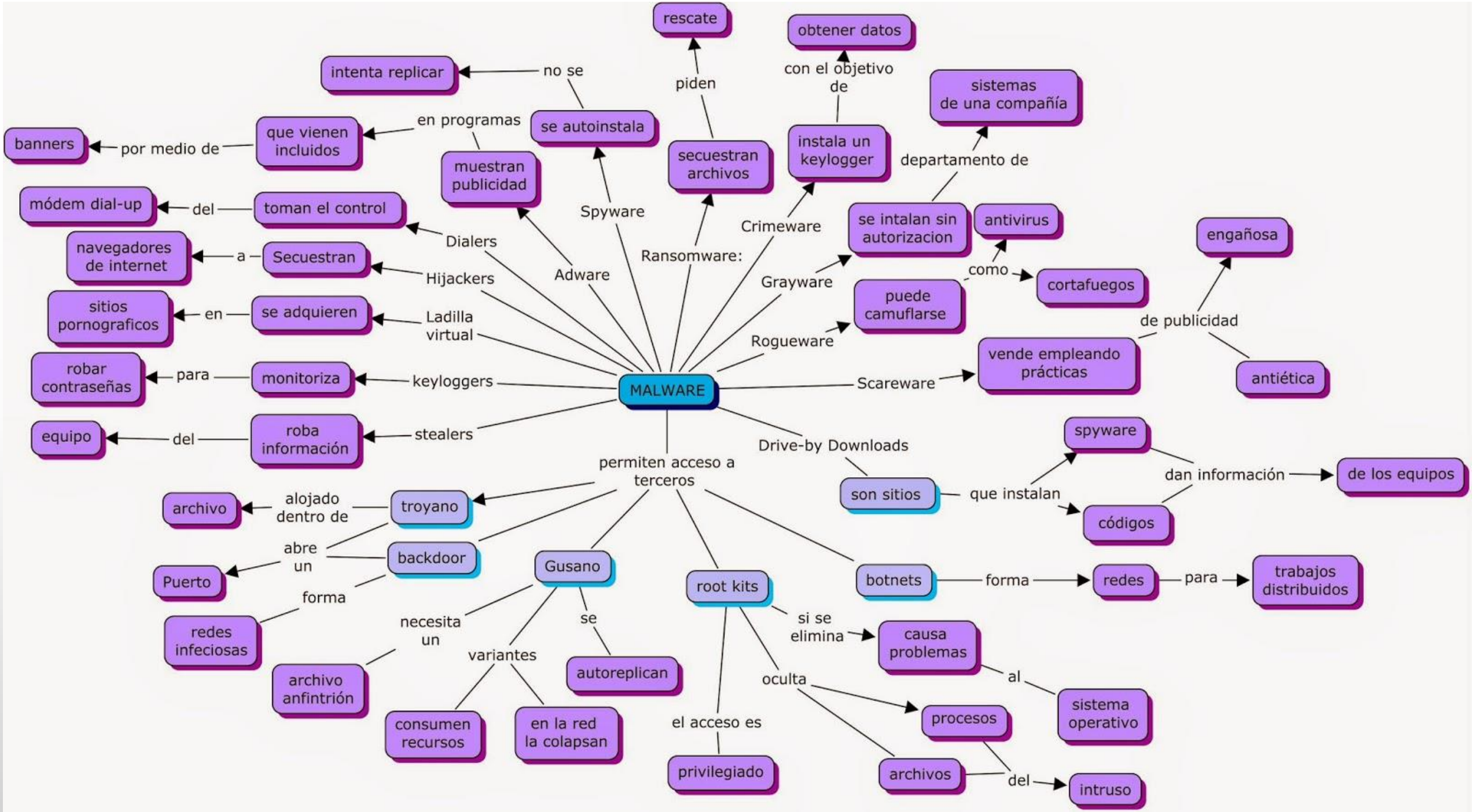
Virus: solo pueden existir en un equipo dentro de otro fichero (.exe, .src, .com, .bat, .doc...), al que modifican añadiendo el código malicioso. Intentan infectar archivos que se ejecutan automáticamente al iniciar el sistema para estar siempre en memoria y continuar su propagación infectando archivos de las mismas características.

Gusano (worms): no necesitan alojarse en otro fichero. Suelen modificar ciertos parámetros del sistema para ejecutarse al inicio del sistema para quedar residentes y realizar el máximo número de copias posible de sí mismos para facilitar su propagación por la red (correo electrónico, redes de compartición de ficheros (P2P), chats...).

Troyano (trojan): pequeña aplicación escondida en otros programas cuya finalidad es disponer de una puerta de entrada al ordenador para que otro usuario o aplicación recopile información o tome el control absoluto del equipo.

CLASIFICACIÓN DEL MALWARE SEGÚN SUS ACCIONES

Puerta trasera (backdoor): es un programa que se introduce en el ordenador de manera encubierta, aparentando ser inofensivo. Establece una "puerta trasera" a través de la cual es posible controlar el ordenador afectado: eliminar archivos o todo el disco duro, capturar y reenviar datos confidenciales o abrir puertos para el control remoto.
Espía (spyware): roba información del equipo para enviarla a un servidor remoto: hábitos de uso del ordenador, páginas visitadas en Internet, información confidencial como nombres de usuario y contraseñas o datos bancarios.
Dialers: actúa cuando el usuario accede a Internet realizando llamadas a números de alto coste, provocando un considerable aumento en la factura telefónica del usuario afectado. Actualmente en desuso porque sólo funcionan si la conexión a Internet se hace a través del módem.
Secuestradores (Ransomware): son programas que cifran los archivos importantes para el usuario, haciéndolos inaccesibles y piden que se pague un rescate para recibir la contraseña y recuperar los archivos. También amenazan con supuestos delitos cometidos (pornografía infantil, piratería...) solicitando el pago de una multa.
Adware y Popups : software que muestra publicidad, empleando cualquier tipo de medio: ventanas emergentes, banners, cambios en la página de inicio o de búsqueda del navegador, etc.
Cookies: no son amenazas en sí. Son pequeños archivos de texto que el navegador almacena en nuestro ordenador con información sobre el uso de Internet (páginas web visitadas, datos del usuario...) que puede ser enviada a terceros sin su consentimiento con la consiguiente amenaza para la privacidad.
Spam: envío de correo electrónico publicitario de forma masiva a cualquier dirección de correo electrónico existente. Tiene como finalidad vender sus productos.
Pharming: redireccionan y suplantan páginas web que se suele utilizar el robo de datos personales y/o bancarios de los usuarios y cometer delitos económicos.
Phishing: envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario. Suelen incluir un enlace que lleva a páginas web falsificadas para que el usuario introduzca la información solicitada que, en realidad, va a parar a manos del estafador.
Redes zombi (botnet): conjuntos de ordenadores que permite al atacante controlar dichas maquinas sin tener acceso físico a ellas y sin el conocimiento del propietario para realizar acciones ilegitimas o ilegales. Existen redes zombi de unos pocas maquinas hasta redes muy grandes (cientos de miles o millones de ordenadores).
Bulo (Hoaxes): son mensajes de correo electrónico engañosos, difundidos masivamente por Internet para sembrar la alarma sobre supuestas infecciones víricas y amenazas contra los usuarios. Aparentan ser ciertos y proponen una serie de acciones a realizar para librarse de la supuesta infección.
Broma (Jokes): tampoco es un virus, sino un programa inofensivo que simula las acciones de un virus informático en nuestro ordenador. Su objetivo no es atacar, sino gastar una broma a los usuarios, haciéndoles creer que están infectados por un virus y que se están poniendo de manifiesto sus efectos.


MALWARE
Adware
intenta replicar
no se
se autoinstala
en programas
que vienen incluidos
por medio de
banners
muestran publicidad
Spyware
Dialers
toman el control
del
módem dial-up
Hijackers
Secuestran
a
navegadores de internet
Ladilla virtual
se adquieren
en
sitios pornograficos
keyloggers
monitoriza
para
robar contraseñas
stealers
roba información
del
equipo
Ransomware:
rescate
piden
secuestran archivos
Crimeware
obtener datos
con el objetivo de
instala un keylogger
Grayware
se intalan sin autorizacion
departamento de
sistemas de una compañía
antivirus
como
cortafuegos
Rogueware
puede camuflarse
Scareware
vende empleando prácticas
de publicidad
engañosa
antiética
Drive-by Downloads
son sitios
que instalan
spyware
códigos
dan información
de los equipos
permiten acceso a terceros
troyano
alojado dentro de
archivo
backdoor
abre un
Puerto
forma
redes infeciosas
Gusano
necesita un
archivo anfintrión
variantes
consumen recursos
se
autoreplican
en la red la colapsan
root kits
el acceso es
privilegiado
si se elimina
causa problemas
al
sistema operativo
oculta
procesos
archivos
del
intruso
botnets
forma
redes
para
trabajos distribuidos

PLAN DE CONTINGENCIAS

Un plan de contingencia o también llamado plan de recuperación de desastres, permite controlar la situación, realizar las actividades necesarias y medidas a tomar para recuperar el sistema. Esta metodología se puede resumir en 8 fases:

1. **Planificación:** preparación y aprobación de esfuerzos y costos.
2. **Identificación de riesgos:** funciones y flujos del proceso de la empresa.
3. **Identificación de soluciones:** Evaluación de Riesgos de fallas o interrupciones.
4. **Estrategias:** Otras opciones, soluciones alternativas, procedimientos manuales.
5. **Documentación del proceso:** Creación de un manual del proceso.
6. **Realización de pruebas:** selección de casos soluciones que probablemente funcionen.
7. **Implementación:** creación de las soluciones requeridas, documentación de los casos.
8. **Monitoreo:** Probar nuevas soluciones o validar los casos.


Análisis de Riesgos
Plan de Recuperación
Estrategias
Procedimientos
Pruebas/ Formación
Mantenimiento Anual
Plan de Contingencias

ENLACES DE SEGURIDAD

[Un informático en el lado del mal.]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Agencia Española de protección de datos

Instituto nacional de ciberseguridad

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

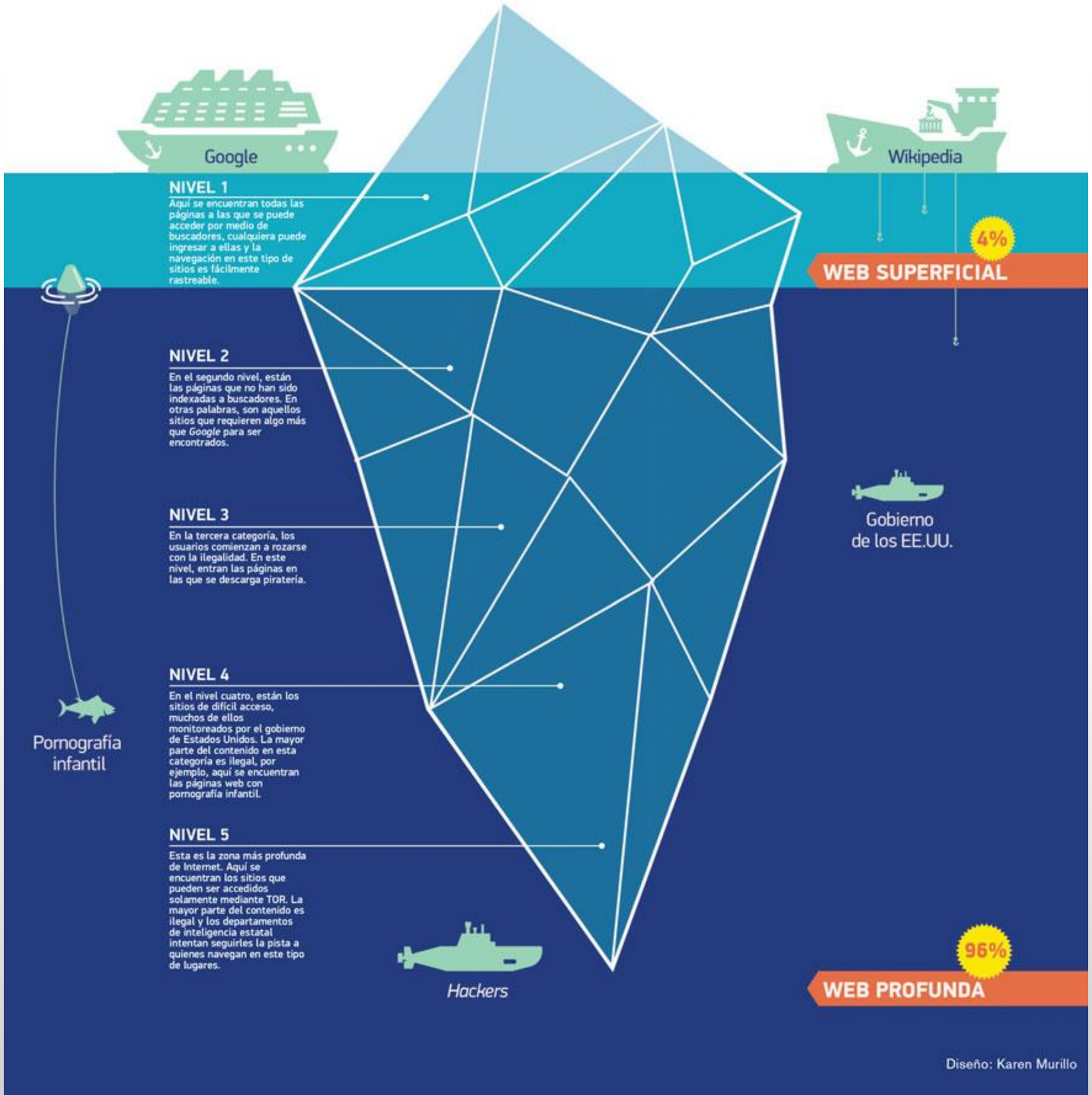
Glosario Ciberseguridad

CCN-CERT
centro criptológico nacional

Reglamento general de protección de datos europeo

PantallasAmigas
desde 2004

DEEP WEB


Google
Wikipedia
NIVEL 1
Aquí se encuentran todas las páginas a las que se puede acceder por medio de buscadores, cualquiera puede ingresar a ellas y la navegación en este tipo de sitios es fácilmente rastreable.
4%
WEB SUPERFICIAL
NIVEL 2
En el segundo nivel, están las páginas que no han sido indexadas a buscadores. En otras palabras, son aquellos sitios que requieren algo más que Google para ser encontrados.
NIVEL 3
En la tercera categoría, los usuarios comienzan a rozarse con la ilegalidad. En este nivel, entran las páginas en las que se descarga piratería.
Gobierno de los EE.UU.
NIVEL 4
En el nivel cuatro, están los sitios de difícil acceso, muchos de ellos monitoreados por el gobierno de Estados Unidos. La mayor parte del contenido en esta categoría es ilegal, por ejemplo, aquí se encuentran las páginas web con pornografía infantil.
Pornografía infantil
NIVEL 5
Esta es la zona más profunda de Internet. Aquí se encuentran los sitios que pueden ser accedidos solamente mediante TOR. La mayor parte del contenido es ilegal y los departamentos de inteligencia estatal intentan seguirles la pista a quienes navegan en este tipo de lugares.
Hackers
96%
WEB PROFUNDA
Diseño: Karen Murillo

AMENAZA EN LA RED

ATAQUES COMO EL QUE PADECIÓ SONY O UNA FUNDIDORA DE ACERO ALEMANA, DAÑADA POR PIRATAS INFORMÁTICOS, HAN DESATADO UNA ALERTA SIN PRECEDENTES EN LA RED: LO QUE ERA SEGURO YA NO LO ES, AQUELLO QUE CREEMOS PRIVADO PUEDE SER PÚBLICO EN CUALQUIER MOMENTO. ¡INTERNET HA ENTRADO EN UNA NUEVA ERA.

POR MIGUEL GALLARDO + GUILLERMO ALTARES


CHRIS ES UN 'BLACKHAT', UN 'HACKER' GUAPERAS Y HONRADO QUE MANEJA A LAS CHICAS Y LAS ARMAS CON IGUAL DESTREZA.
PERO EL BUEN 'HACKER' QUE HA POPULARIZADO HOLLYWOOD TIENE POCO QUE VER CON LOS 'HACKERS' DE VERDAD.
ESTAMOS HABLANDO DE REDES INTERNACIONALES DE DELINCUENCIA QUE SOLO EN EL AÑO 2013 ROBARON ALREDEDOR DE 400.000 MILLONES DE DÓLARES.
EL 40% DE LAS COMPAÑÍAS HAN SUFRIDO ALGÚN TIPO DE CIBERATAQUE.
HEMOS PASADO DE UNA ÉPOCA ROMÁNTICA EN LA QUE LOS 'HACKERS' ERAN UNA ESPECIE DE ROBIN HOOD A VERDADERAS BANDAS DE CRIMEN ORGANIZADO...
CADA AÑO MILLONES DE PERSONAS SON VÍCTIMAS DE NUMEROSOS ROBOS DE DATOS. LOS 'HACKERS' VENDEN LA INFORMACIÓN BANCARIA DE LOS USUARIOS EN PÁGINAS WEB ILEGALES.
EN ESPAÑA SE PRODUCEN MÁS DE 70.000 ATAQUES INFORMÁTICOS AL AÑO, SEGÚN LA POLICÍA. LAS PÉRDIDAS ANUALES POR ROBO SON DE 482 MILLONES DE EUROS.

EL 24 DE NOVIEMBRE DE 2014, SONY SUFRIÓ UN ATAQUE MASIVO QUE EXPUSO MÁS DE 12.000 'E-MAILS' E INFORMACIÓN SENSIBLE DE LA COMPAÑÍA.

ENTRE LOS DATOS FILTRADOS ESTABAN LOS SUELDOS DE LOS GRANDES EJECUTIVOS, DOCUMENTOS DE DESPIDO, PRESUPUESTOS, GUIONES Y MÁS DE 3.800 NÚMEROS DE LA SEGURIDAD SOCIAL.

LOS 3.500 EMPLEADOS DE SONY VIERON ESTA IMAGEN NADA MÁS ENCENDER SU ORDENADOR, TODOS RECIBIERON INSTRUCCIONES PARA DESCONECTARSE DE LA RED. EL FBI ACUSÓ DEL ATAQUE A COREA DEL NORTE.

LO CIERTO ES QUE LOS ATAQUES SON CADA VEZ MÁS IMAGINATIVOS Y CONTRA OBJETIVOS MÁS IMPORTANTES, PESE A LAS CORTAPISAS QUE PONEN LAS EMPRESAS DE SEGURIDAD INFORMÁTICA.

A FINALES DE 2013, UN CAJERO AUTOMÁTICO EN KIEV EMPEZÓ A ENTREGAR DINERO A HORAS DEL DÍA AL AZAR. NADIE HABÍA INSERTADO UNA TARJETA.

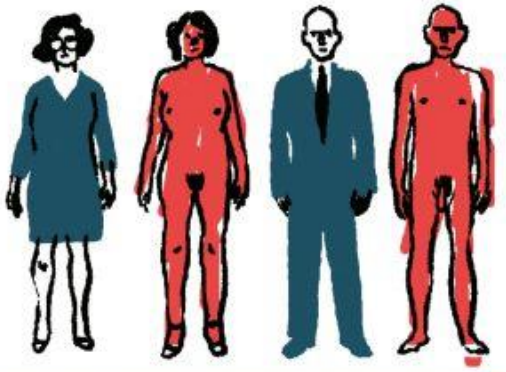
ERA CARBANAK, UN SOFISTICADO ATAQUE QUE AFECTÓ A ENTIDADES FINANCIERAS EN MÁS DE 30 PAISES. LOS PIRATAS TARDABAN ENTRE DOS Y CUATRO MESES EN HACERSE CON EL DINERO.

CÓMO FUNCIONA CARBANAK: BASTA CON QUE UN EMPLEADO ABRA UN ADJUNTO DE UN CORREO, COMO UN DOCUMENTO WORD, PARA QUE SE DESATE UN MECANISMO DE ESPIONAJE E INFECCIÓN QUE PERMITE A LOS 'HACKERS' CONTROLAR EL EQUIPO SIN QUE EL USUARIO SE DÉ CUENTA Y QUE ACABA CON EL ROBO DE MILES DE MILLONES.

LOS MÉTODOS DE DEFENSA NO SON INFALIBLES. LAS COMPAÑÍAS Y LOS INDIVIDUOS SIGUEN SIENDO VULNERABLES. TODOS NOSOTROS PODEMOS SER VÍCTIMAS DE UN ATRACO EN EL CIBERESPACIO.

EN 2015 LOS 'HACKERS' SE HICIERON CON LOS DATOS DE LA EMPRESA DE SEGUROS MÉDICOS ANTHEM.

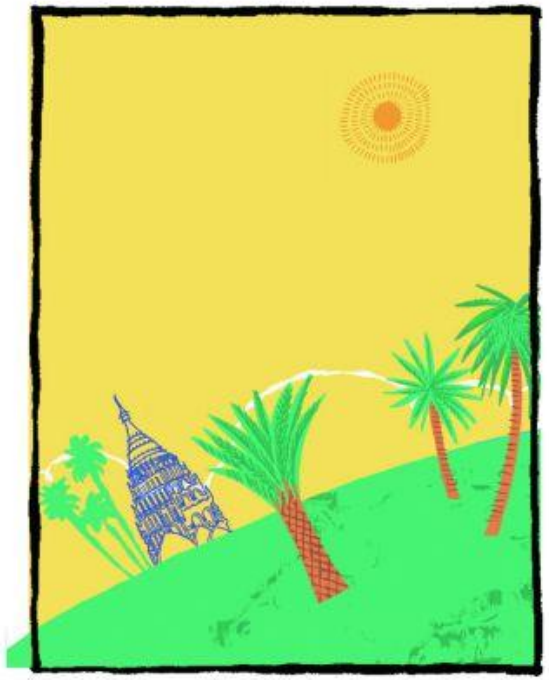
LOS HISTORIALES DE 78,8 MILLONES DE PERSONAS QUEDARON EXPUESTOS. DATOS TAN SENSIBLES COMO LOS MÉDICOS.



JPMORGAN CHASE SUFRIÓ EL VERANO PASADO UNA INTRUSIÓN MASIVA EN SU SISTEMA INFORMÁTICO QUE AFECTÓ A 76 MILLONES DE HOGARES.

LOS PIRATAS INFORMÁTICOS TUVIERON ACCESO A LOS DATOS DE CONTACTO DE SUS CLIENTES, COMO CORREOS ELECTRÓNICOS Y TELÉFONOS. LAS PRIMERAS INFORMACIONES INDICABAN QUE HABÍA AFECTADO A CERCA DE UN MILLÓN DE CUENTAS.

SIN EMBARGO, EL ALCANCE FUE MAYOR, PORQUE AFECTÓ A TODOS LOS USUARIOS DE SU PORTAL O SU APLICACIÓN PARA MÓVILES.




ACTUALMENTE UNOS 3.000 MILLONES DE PERSONAS ESTÁN CONECTADAS A INTERNET. UN 40% DE LA POBLACIÓN MUNDIAL...


PERO PARA FINALES DE 2015... 5.000 MILLONES ESTARÁN VINCULADAS A LA RED CON TODO TIPO DE DISPOSITIVOS...

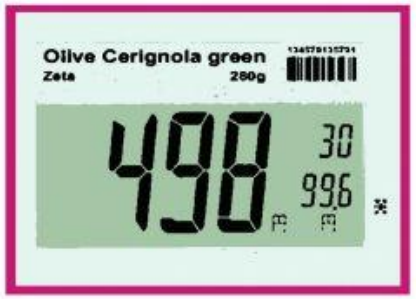

AHORA SERÁN LAS COSAS LAS QUE ESTÉN UNIDAS ENTRE SÍ Y A LA RED: NEVERAS, TELEVISIONES, SUPERMERCADOS, CALEFACCIONES...


... COCHES, CUALQUIER TIPO DE DISPOSITIVO CONECTADO A UNA RED PUEDE VERSE COMPROMETIDO POR UN TERCERO.


ACTUALMENTE, EL DAÑO DE LOS CIBERATAQUES NO ES SOLO VIRTUAL. TAMBIÉN PUEDE SER FÍSICO.

VENIMOS DE HACER PRUEBAS DE SEGURIDAD PARA UNOS CENTROS COMERCIALES...

LAS BÁSCULAS SON ELECTRÓNICAS Y LAS ETIQUETAS DE LOS PRECIOS YA SON DE PAPEL ELECTRÓNICO...



LAS CÁMARAS FRIGORÍFICAS TIENEN UNA INTERFAZ WEB.

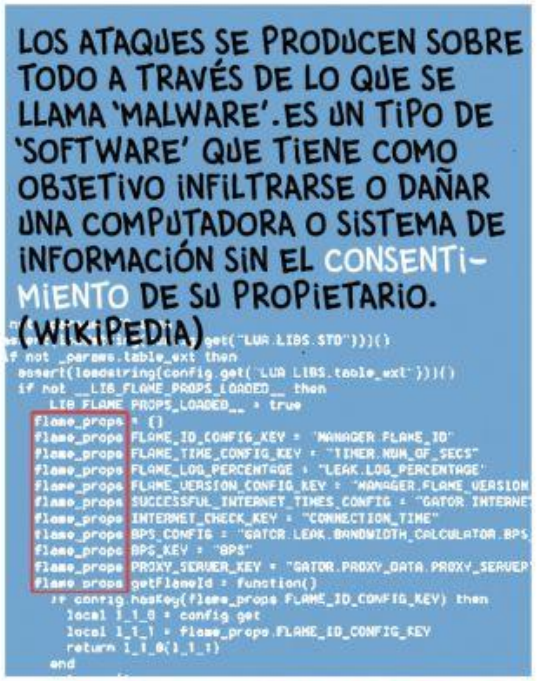
AHORA ES MUCHO MÁS CARO HACER SEGUROS ESE TIPO DE DISPOSITIVOS.

ALGUIEN CON UN MÓVIL O CON UN PORTÁTIL PODRÍA CAMBIAR LOS PRECIOS EN UN SUPERMERCADO Y LOS AJUSTES EN LOS APARATOS.

¿Y SI EN VEZ DE UN CENTRO COMERCIAL FUERA UNA PLANTA POTABILIZADORA O UNA CENTRAL NUCLEAR?


CUALQUIER COSA PUEDE SUCEDER: HACE POCO TIEMPO, EL 9 DE ABRIL DE 2015, UNOS 'HACKERS' DEL ESTADO ISLÁMICO PARARON UNA EMISIÓN DE LA TELEVISIÓN FRANCESA...
i love you isis


TODOS ESTAMOS EXPUESTOS.
TV5MONDE
CyberCaliphate
i love you isis


LOS ATAQUES SE PRODUCEN SOBRE TODO A TRAVÉS DE LO QUE SE LLAMA 'MALWARE'. ES UN TIPO DE 'SOFTWARE' QUE TIENE COMO OBJETIVO INFILTRARSE O DAÑAR UNA COMPUTADORA O SISTEMA DE INFORMACIÓN SIN EL CONSENTIMIENTO DE SU PROPIETARIO. (WIKIPEDIA)

MALWARE


BÁSICAMENTE EL 'MALWARE' INTRODUCE UN PROGRAMA EN NUESTRO SISTEMA, CON LO CUAL PERDEMOS EL CONTROL SOBRE ÉL.


TAMBIÉN ESTÁN LOS ATAQUES DE DENEGACIÓN DE SERVICIOS QUE CAUSAN QUE UNA PRESTACIÓN O RECURSO SEA INACCESIBLE A LOS USUARIOS LEGÍTIMOS.


Y LUEGO LA HABILIDAD DE LOS 'HACKERS' PARA ENTRAR TRANQUILAMENTE EN NUESTROS SISTEMAS.

NUESTROS ORDENADORES SE CONVIERTEN EN ZOMBIS QUE, TRAS SER INFECTADOS, PUEDEN SER USADOS POR UNA TERCERA PERSONA.

EN AGOSTO DE 2011 EXISTÍAN ENTRE 100 Y 150 MILLONES DE EQUIPOS COMPROMETIDOS EN EL MUNDO.

LOS PRINCIPALES ATAQUES INFORMÁTICOS TIENEN SU ORIGEN EN CHINA Y RUSIA.

UNA INTERVENCIÓN DE INTERPOL CONTRA SIMDA BOTNET, UN 'MALWARE' PERNICIOSO, SACÓ A LA LUZ QUE EN LOS DOS PRIMEROS MESES DEL AÑO SE HABÍAN PRODUCIDO UNAS 90.000 INFECCIONES EN 190 PAÍSES.

LA OPERACIÓN FUE REALIZADA POR UNA NUEVA RAMA DE INTERPOL: INTERPOL GLOBAL COMPLEX FOR INNOVATION, EN COLABORACIÓN CON MICROSOFT, KASPERSKY LAB, TREND MICRO Y EL INSTITUTO JAPONÉS PARA LA CIBERDEFENSA.

INTERPOL

TAMBIÉN PARTICIPARON EL INSTITUTO NEERLANDÉS DE CRÍMENES TECNOLÓGICOS, EL FBI Y LA POLICÍA DE LUXEMBURGO. LA MAGNITUD DE LA OPERACIÓN PERMITIÓ LOCALIZAR SERVIDORES EN HOLANDA, EE UU, LUXEMBURGO Y POLONIA.


ENTRE MARZO DE 1989 Y DICIEMBRE DEL 1990, EL INGLÉS TIM BERNERS-LEE, CON AYUDA DEL BELGA ROBERT CAILLIAU, DESARROLLÓ LA PRIMERA IDEA DE UNA RED INFORMÁTICA MUNDIAL.
WWW


LA WWW NOS PROMETÍA UN FUTURO IDÍLICO EN EL QUE TODOS ESTARÍAMOS CONECTADOS: LA WEB ES EL MEDIO DE MAYOR INTERCAMBIO PERSONAL EN LA HISTORIA DE LA HUMANIDAD, NOS DECÍAN.


PODRÍAMOS COMPRAR Y HACER NEGOCIOS SENTADOS TRANQUILAMENTE EN NUESTRA CASA. UN MEDIO BARATO Y SEGURO.


TOTALMENTE
SEGURO


...BLINDADO POR UN SISTEMA DE CONTRASEÑAS Y USUARIOS. IMPERMEABLE A ROBOS Y SUPLANTACIONES DE IDENTIDAD.


PERO AHORA SABEMOS QUE ESO NO ES VERDAD. ALGUIEN CON UNOS POCOS CONOCIMIENTOS EN INFORMÁTICA PUEDE COLARNOS UN TROYANO PARA INSTALARNOS 'SOFTWARE' DE REGISTRO DE PULSACIONES EN EL TECLADO Y VIGILAR TODO LO QUE ESCRIBE EL USUARIO: NOMBRES Y CONTRASEÑAS PARA ENTRAR EN CUENTAS BANCARIAS.

EL 23/12/2014, DINAHOSTING, UNA PEQUEÑA COMPAÑÍA GALLEGA DE ALOJAMIENTO, SUFRIÓ UN DURO ATAQUE DDOS QUE DEJÓ SIN SERVICIO A MÁS DE 60.000 USUARIOS.

DINAHOSTING#G&G%GSG$GYU
DINAH=STIN#G&5%TSX$(YU)
D#N&H=STIN#G&5%TSX$(YU)

UN ATAQUE DDOS NO ROBA DATOS NI ATENTA CONTRA LA SEGURIDAD, LO ÚNICO QUE HACE ES INUNDAR LOS SERVIDORES CON PETICIONES UTILIZANDO ORDENADORES ZOMBIS.

DINAHOSTING RECIBIÓ VARIAS OLEADAS DE ATAQUES DESDE LAS CINCO DE LA TARDE HASTA LAS SIETE DE LA MAÑANA DEL DÍA SIGUIENTE.

LAS GRANDES CORPORACIONES Y LOS BANCOS INVIERTEN DINERO EN SEGURIDAD, PERO NO PASA LO MISMO CON OTRAS EMPRESAS QUE NO ESTÁN RELACIONADAS DE UNA FORMA DIRECTA CON FONDOS ECONÓMICOS.

NO EXISTEN SISTEMAS INFORMÁTICOS SEGUROS AL 100%, SOLO SISTEMAS CUYOS FALLOS AÚN NO HAN SIDO DESCUBIERTOS.

TENEMOS QUE CAMBIAR LA IDEA DE LA PRIVACIDAD. ESTAMOS MUCHO MÁS EXPUESTOS DE LO QUE PENSAMOS.

TODA NUESTRA VIDA ESTÁ EN INTERNET.

FUENTES: INCIBE (INSTITUTO NACIONAL DE CIBERSEGURIDAD), KASPERSKY, THIBER, S21SEC, HACKING TEAM, SYMANTEC, MINISTERIO DEL INTERIOR, INTERPOL, 'THE NEW YORK TIMES', 'EL PAÍS', 'WIRED'.

ENTREVISTAS A EXPERTOS:
JOSÉ ALEMÁN (S21SEC)
ERIC RABE HACKING TEAM
ADOLFO HERNÁNDEZ (THIBER)