

Módulo 7

Seguridad Informática



ECDL

Seguridad Informática

- Conceptos de seguridad
- Malware
- Seguridad de la red
- Uso seguro del Web
- Comunicaciones
- Gestión de datos seguros



Conceptos de seguridad

- Amenazas para los datos
- Valor de la información
- Seguridad personal
- Seguridad de un archivo

Conceptos de seguridad

(Amenazas para los datos)

Diferencias entre datos e información

Dato	Información
Representación simbólica	Conjunto de datos procesados
No tiene sentido semántico	Tiene un significado
No transmite mensaje	Transmite un mensaje
No incrementa el conocimiento	Incrementa el conocimiento

Conceptos de seguridad

(Amenazas para los datos)



- Delito informático
- Ejemplos: sabotaje informático, piratería informática, robo de identidad,...
- Hackear
- Crackear
- Hacking ético



Conceptos de seguridad

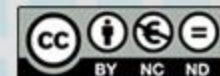
(Amenazas para los datos)

- Amenazas humanas
- Amenazas de hardware
- Amenazas de software
- Amenazas de red
- Amenazas por desastres naturales

Conceptos de seguridad

(Valor de la información)

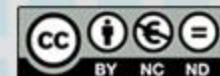
- Hacer copias de seguridad
- Cuidado con la información dada en Internet
 - Datos personales
 - Datos bancarios
 - Ubicación geográfica
 - Fotografías i vídeos



Conceptos de seguridad

(Valor de la información: Prevención)

- Usar contraseñas
- Bloquear el ordenador
- Activar un cortafuegos
- Instalar antivirus
- Encriptar el disco duro
- Equipo no conectado a Internet
- No usar Wi-Fi pública
- No abusar de la nube
- Protocolo "https"
- No aceptar cookies
- Vigilar con el correo electrónico
- Encriptar Chats y correos electrónicos
- Proteger los teléfonos móviles



Conceptos de seguridad

(Valor de la información)

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad

Conceptos de seguridad

(Seguridad personal)

- Ingeniería social:
 - Phishing
 - Shoulder surfing
 - ...
- Robo de identidad:
 - Correos falsos
 - Personal
 - Ataque organizado

Conceptos de seguridad

(Seguridad de un archivo)

- Macros
- Establecer una contraseña
 - Ocho caracteres, como mínimo
 - NO: datos personales o de la empresa
 - NO: una palabra completa
 - Diferente de otras contraseñas anteriores
 - Ha de contener diferentes tipos de caracteres: letras mayúsculas y minúsculas, números y símbolos



Conceptos de seguridad

(Seguridad de un archivo)

- Cifrado
- Compresión de archivos
- Proteger un archivo con su aplicación
- Keyloggers

Malware

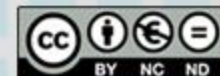
- Definición, función y tipos
- Protección



Malware

(Definición, función y tipos)

- Virus informáticos
- Gusanos
- Troyano informático
- Backdoor (puerta trasera)
- Spyware (Software espía)
- Exploit
- Rootkit (herramienta de intrusión)
- Ransomware



Malware

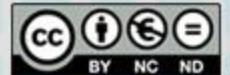
(Protección: Virus)

- Creación
- Contagio
- Incubación
- Replicación
- Ataque

Malware

(Protección: Síntomas de la presencia de virus)

- Se hace más lento el trabajo o se cuelga demasiado
- El disco duro trabaja más de la cuenta
- El sistema no arranca o se reinicia sólo
- Algunos programas no se pueden ejecutar
- Reducción espacio en discos
- El sistema no reconoce alguna unidad de disco
- Se reduce la memoria disponible
- Aparecen mensajes extraños
- La pantalla se borra o cambia
- Aumenta el tamaño de los archivos o no se pueden abrir
- Aparecen o desaparecen algunos archivos
- En algunos archivos aparece información de otros archivos



Malware

(Protección: Antivirus)

Objetivos básicos:

- Detectar
- Desinfectar
- Proteger

Actuación:

- Inspecciona los correos
- Monitoriza los archivos
- Inspecciona periódicamente todo el ordenador

Limitaciones:

- Spam
- Ataques directos de un hacker
- Actividades criminales online

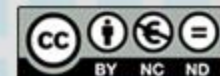


CDL



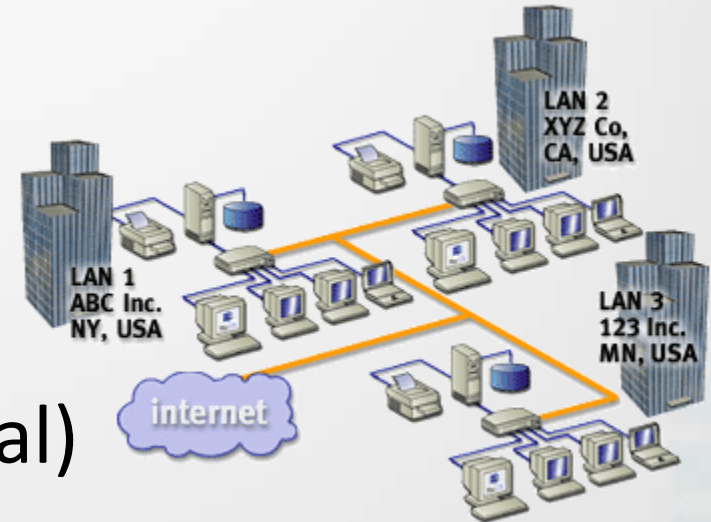
Seguridad de la red

- Redes
- Conexiones de red
- Seguridad inalámbrica



Seguridad de la red

(Redes)



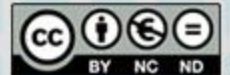
- LAN (redes de área local)
- WAN (redes de área amplia)

Seguridad de la red

(Redes: Administradores de red)

Funciones del administrador de red:

- Diseño i seguridad de la red.
- Proporcionar soporte.
- Administrar las cuentas de usuario.
- Administrar el espacio en discos y mantener copias de seguridad .
- Asegurarse de que la red se utiliza eficientemente.
- Asignar direcciones.
- Configuración de autenticación y autorización.
- Mantenimiento de los servidores, las instalaciones de red y los detectores de intrusos.



Seguridad de la red

(Redes: Firewall)



Ventajas:

- Protege de intrusiones
- Protege la información privada
- Optimiza el acceso

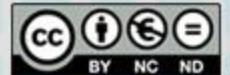
Limitaciones:

- Traidores corporativos
- Ataques de la ingeniería social
- Ataques de virus informáticos a través de archivos y software
- Errores de seguridad de los servicios que se publiquen en Internet

Seguridad de la red


(Conexiones de red)

- Red Telefónica Conmutada (RTC)
- Línea de Abonado Digital Asimétrica (ADSL)
- Cable
- Vía satélite
- Wi-Fi
- Conexión móvil (4G)



Seguridad de la red

(Seguridad inalámbrica: Wi-Fi)

- Botón “Acceso a Internet”: 
- Conectar
- Clave de la red

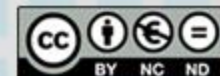


- Configuración: “Abrir Centro de redes”

Seguridad de la red

(Seguridad inalámbrica: Tipos de seguridad)

- Acceso protegido Wi-Fi
 - WPA
 - WPA2
- Autenticación 802.1x

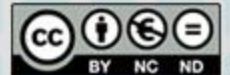


Seguridad de la red

(Seguridad inalámbrica: Direcciones MAC)

Funciones:

- Controlar el acceso al medio físico de transmisión
- Añadir la dirección MAC de los nodos fuente y destino
- Al transmitir en origen, delimitar las tramas de red para que el receptor reconozca el inicio y final de cada trama
- Al recibir en destino, determinar el inicio y final de una trama de datos
- Efectuar detección y corrección de errores de transmisión
- Descartar tramas duplicadas o erróneas

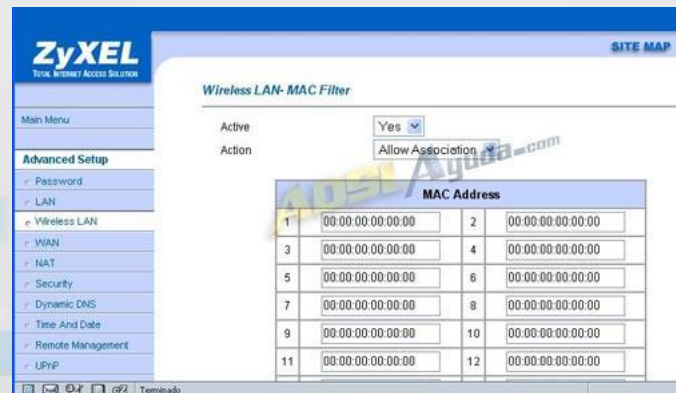


Seguridad de la red

(Seguridad inalámbrica: Direcciones MAC)

Introducir las direcciones MAC de vuestros equipos:

- Desconectad el router de la línea telefónica
- Conectad el router, con cable Ethernet, al ordenador
- Abrid el navegador y escribid la IP del router
- Aparecerá la página de configuración del router. Buscad el apartado *Wireless LAN – MAC Filter*
- Escribid las direcciones MAC de vuestros equipos

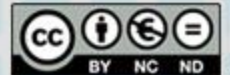


Seguridad de la red

(Seguridad inalámbrica: Riesgos de una red sin protección)

Precauciones:

- Uso de una red privada virtual (VPN)
- Uso de conexiones SSL
- Desactivación del uso compartido
- Mantener la opción Wi-Fi desactivada cuando no la necesitemos
- Solución de seguridad en Internet sólida



Seguridad de la red

(Seguridad biométrica)

Sistemas de autenticación:

- Uso de contraseña
- Uso de tarjetas
- Reconocimiento físico del usuario

Uso seguro del Web

- Sitios Web seguros y Certificación digital
- Pharming
- Contraseña de un sólo uso
- Autocompletado en un formulario
- Cookies
- Software para controlar contenidos de Internet
- Redes sociales



Uso seguro del Web

(Sitios Web seguros)

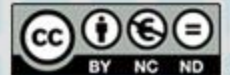
- <http://www.uab.es>
- <https://www.uab.es>
- La información se envía cifrada
- Autoridad de certificación (CA)
- Certificados SSL
 - Confidencialidad
 - Integridad
 - Autenticación
- Firma digital



Uso seguro del Web

(Pharming)

- Pharming: Redirigir a otra página
- Dirección IP / Nombre de Dominio
- Ataque: directamente a los servidores DNS o a ordenadores concretos
- Combatir el pharming:
 - Software especializado de protección DNS
 - Uso de addons para los navegadores web
- Observar dónde nos dirige una dirección:
 - Comando traceroute (UNIX, MAC i GNU/Linux)
 - Comando tracert (Windows)



Uso seguro del Web

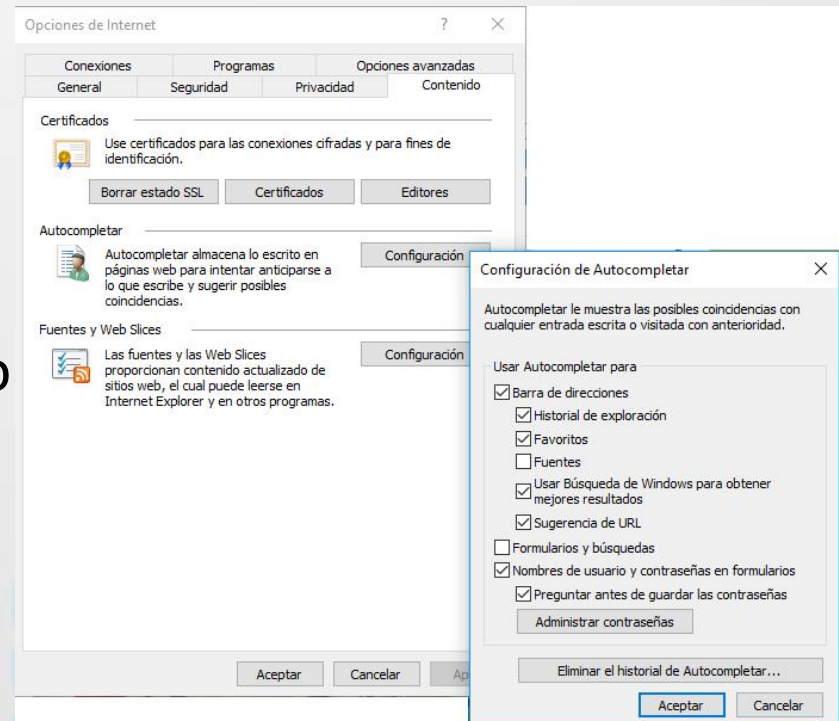
(Contraseña de un sólo uso)

- OTP: One-Time Password
 - Ventaja: no es vulnerable a ataques de REPLAY
 - Inconveniente: no podemos memorizar todas las contraseñas posibles

Uso seguro del Web

(Autocompletar en un formulario)

- Activar o desactivar Autocompletar (IE Explorer):
 - Menú o botón “Herramientas”: opción “Opciones de Internet”.
 - Ficha “Contenido”: botón “Configuración” (apartado Autocompletar).



Uso seguro del Web

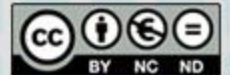
(Cookies)

- Según la entidad que las gestiona:
 - Propias
 - De terceros
- Según el tiempo que permanecen activadas:
 - De sesión
 - Persistentes
- Según su finalidad:
 - Técnicas
 - De personalización
 - De análisis

Uso seguro del Web

(Control parental)

- Controlar el tiempo de uso y el contenido al que se accede
- Hasta Windows 8: panel de control *Control parental*
- Windows 10:
 - Hay que tener cuenta Microsoft
 - Configuración inicial:
<https://account.microsoft.com/family/about>
 - Administrar (Inicio - Configuración - Cuentas)



Uso seguro del Web

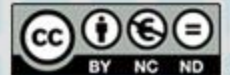
(Redes sociales)

- Ejemplos: Facebook, Twitter, Wikipedia, Windows Live Messenger,...
- Objetivos:
 - Intercambiar información
 - Ofrecer apoyo
 - Conversar y socializar de manera informal
 - Debatir

Uso seguro del Web

(Redes sociales: Precauciones)

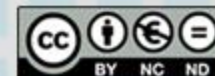
- Mantened actualizado vuestro sistema operativo, navegador y antivirus
- Cuidad vuestra privacidad
- Evitad contactar con extraños
- No suplantéis la identidad
- No ofendáis ni compartáis contenidos inapropiados
- Pensad bien antes de subir una foto



Uso seguro del Web

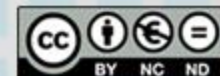
(Redes sociales: Peligros)

- Cyberbullying / Grooming
- Incitación al odio
- Rechazo laboral
- Phishing
- Malware
- Problemas de privacidad
- Pérdida de productividad



Comunicaciones

- Correo electrónico
- Mensajería instantánea

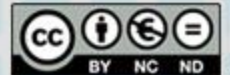


Comunicaciones

(Correo electrónico: Cifrar/Descifrar)

- Cifrado asimétrico:

- El remitente tendrá 2 claves únicas. Una pública y otra privada.
- El destinatario también tendrá 2 claves únicas. Una pública y otra privada.
- Ni el destinatario ni el remitente proporcionarán a terceros su clave privada.
- El destinatario y el remitente distribuirán públicamente su clave pública.
- El remitente, una vez escrito el mensaje, lo cifrará con la clave pública del destinatario.
- El destinatario no podrá leerlo porque el contenido está cifrado. Para descifrar el mensaje, el destinatario usará su clave privada.



Comunicaciones

(Correo electrónico: Cifrar/Descifrar)

- Microsoft Outlook: extensiones:
GP4Win / Outlook Privacy plugin
- Mozilla Thunderbird: extensiones:
Enigmail / WebPG for Mozilla.
- Navegadores Chrome i Firefox: extensiones:
Mailvelope / Secure Gmail.
- Android: aplicaciones:
k9mail / APG.

Comunicaciones

(Correo electrónico: Firma digital)

<http://firmaelectronica.gob.es/Home/Ciudadanos/Firma-Electronica.html>



Comunicaciones

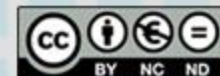
(Correo electrónico: SPAM y Phishing)

- SPAM

- Phishing

Recomendaciones:

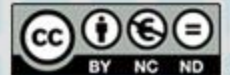
- No responder a correos escritos en otros idiomas
- No responder a correos enviados por entidades de las que no sois cliente
- No responder de forma inmediata a correos que hablen de un sorteo u oferta
- No responder a los que avisen del final de actividades financieras recibidos por sorpresa
- No responder a correos sospechosos sin confirmarlos por teléfono o personalmente
- No entrar en la página web de vuestro banco a través de buscadores
- Y, sobre todo, nunca dar información de vuestras cuentas ni tarjetas por correo electrónico



Comunicaciones

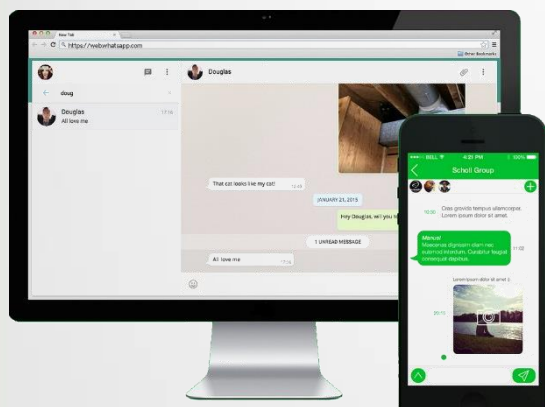
(Correo electrónico: Archivos adjuntos)

- Archivos ejecutables: EXE, COM, BAT,...
- Cualquier tipo de archivo: JPG, DOC, PDF,...
- Medidas de prevención:
 - Disponer de un antivirus actualizado
 - Sospechar de archivos con extensión EXE, COM, BAT, ZIP, SHS o PIF que no esperábamos recibir
 - Sospechar incluso cuando provienen de personas conocidas
 - Antes de abrir un archivo adjunto, mejor descargarlo y analizarlo con nuestro antivirus.

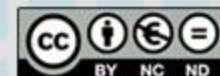


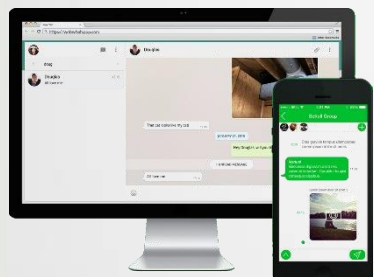
Comunicaciones

(Mensajería instantánea)



- Yahoo! Messenger, Windows Live Messenger (Skype), Google Talk (Hangouts),...
- Facebook Messenger, Skype, Line, Hangouts, Telegram y Whatsapp

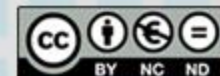




Comunicaciones

(Mensajería instantánea: Precauciones)

- Proteged vuestra identidad
- Utilizad antivirus en cualquier dispositivo
- Tened cuidado con los archivos multimedia
- No deis el número de teléfono de otras personas sin su consentimiento
- No facilitéis información privada
- Eliminad el historial de las conversaciones con frecuencia
- Desconfiad de las redes WiFi públicas
- Mantened siempre actualizada la aplicación



Gestión de datos seguros

- Copia de seguridad de los datos
- Destrucción segura

Gestión de datos seguros

(Copia de seguridad)

- Periodicidad de la realización de las copias
- Definición de la información que debe guardarse
- Ubicación de les copias
- Comprobación de su estado

Gestión de datos seguros

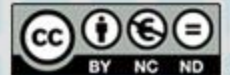
(Copia de seguridad: Seguridad física de los dispositivos)

Amenazas:

- Desastres naturales, incendios accidentales, picos de tensión, ...
- Ataques externos intencionados (robo, sabotaje,...)
- Ataques internos intencionados

Las CS deberían de:

- Estar, como mínimo, duplicadas
- Estar almacenadas, físicamente, lejos de las instalaciones en las que se genera
- Estar almacenadas en medios seguros
- Ser realizadas y comprobadas a menudo



Gestión de datos seguros

(Copia de seguridad: Herramientas)

- Copia de seguridad de archivos
- Copia de seguridad de imagen del sistema
- Versiones anteriores
- Restaurar sistema

Gestión de datos seguros

(Destrucción segura)

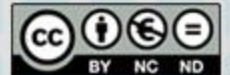
Ley Orgánica de Protección de Datos (LOPD)

Documentación impresa:

- Contratar a una empresa especializada en destrucción de papel
- Triturar el papel
- Quemar el papel

Documentación digital:

- Desmagnetización
- Destrucción
- Sobreescritura



Gestión de datos seguros

(Destrucción segura: niveles de seguridad)

De Nivel Alto:

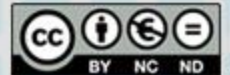
- Datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y los que no se prevé la posibilidad de adoptar el nivel básico
- Datos recogidos con fines policiales sin consentimiento de las personas afectadas
- Datos derivados de actos de violencia de género

Gestión de datos seguros

(Destrucción segura: niveles de seguridad)

De Nivel Medio:

- Datos relativos a la comisión de infracciones administrativas o penales
- Datos que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito)
- Datos de las Administraciones tributarias
- Datos de las entidades financieras
- Datos de las entidades Gestoras y Servicios Comunes de Seguridad Social
- Datos de les mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social
- Datos que ofrezcan una definición de la personalidad y permitan evaluar aspectos de la misma o del comportamiento de las personas
- Datos de los operadores de comunicaciones electrónicas, respecto a los datos de tránsito y localización



Gestión de datos seguros

(Destrucción segura: niveles de seguridad)

De Nivel Básico:

- Cualquier otro archivo que contenga datos de carácter personal
- Archivos que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:
 - Los datos se utilizan para realizar una transferencia dineraria a entidades de las que los afectados sean miembros
 - Archivos no automatizados donde los datos no guarden relación con la finalidad del archivo
 - Archivos que contengan datos de saludo que se refieran exclusivamente al grado o condición de discapacidad con motivo del cumplimiento de deberes públicos

Agencia Española de Protección de Datos: <http://www.agpd.es/>

