OBJETOS DE APRENDIZAJE | 2019

LÍNEA 2

MATERIALES DE FORMACIÓN PARA ESTUDIANTES
DE GRADO DE LA COMPETENCIA DIGITAL

4. Seguridad: 4.1. Protección de dispositivos:

3. Protección de dispositivos

crue Universidades Españolas
Red de Bibliotecas REBIUN

Colección Objetos de Aprendizaje, 2019

MATERIALES DE FORMACIÓN PARA ESTUDIANTES DE GRADO DE LA COMPETENCIA DIGITAL

4. Seguridad: 4.1. Protección de dispositivos:

3. Protección de dispositivos

REBIUN Línea 2 (3er. P.E.) Grupo de Competencia Digital

Seguridad.
Protección de dispositivos.

PROTECCIÓN DE DISPOSITIVOS

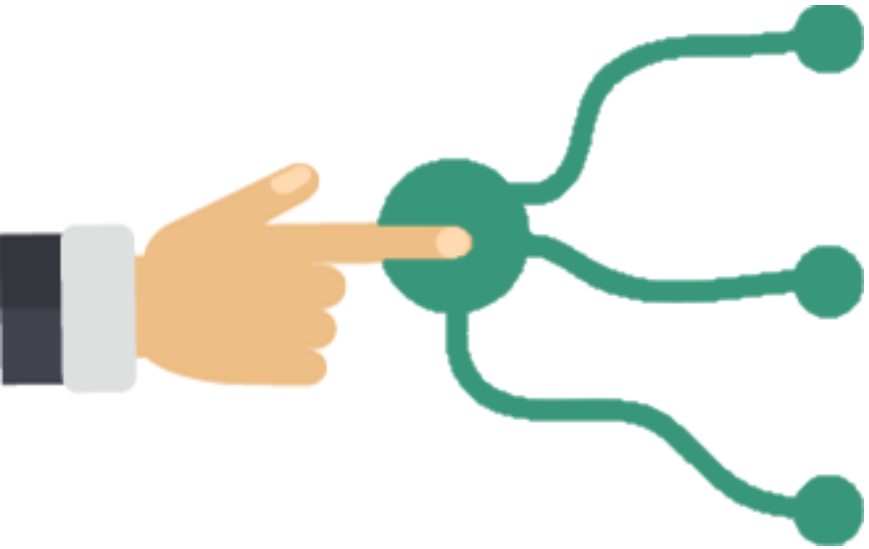
CRUE REBIUN Red de Bibliotecas Universitarias

SUMARIO

- Protección de dispositivos
  - Acceso al dispositivo
  - Sistema operativo
  - Aplicaciones y programas
  - Archivos y carpetas
  - Navegación web
  - Conexiones inalámbricas
  - Geolocalización
  - Sistemas de protección
  - Canales de información
  - Sentido común

OBJETIVOS

Al finalizar esta actividad tienes que ser capaz de:



- Conocer diversas formas de proteger los dispositivos.
- Ser consciente de los riesgos asociados al uso de dispositivos.
- Realizar un uso responsable y seguro de los dispositivos.

PROTECCIÓN DE DISPOSITIVOS

El desarrollo de dispositivos móviles conectados a la red ha cambiado la forma en que trabajamos y nos relacionamos con los demás. Los utilizamos continuamente para navegar, instalar aplicaciones, colaborar en línea o comunicarnos, y los beneficios de su uso son visibles en el día a día.

A través de nuestros móviles, portátiles y demás dispositivos intercambiamos y almacenamos multitud de aplicaciones, archivos e información sensible, por lo que es importante conocer las medidas de protección y seguir las recomendaciones de seguridad básicas para garantizar la protección de los dispositivos.

Se debe prestar especial atención a los siguientes aspectos:

- Acceso al dispositivo
- Sistema operativo
- Aplicaciones y programas
- Archivos y carpetas
- Navegación web
- Conexiones inalámbricas
- Geolocalización
- Sistemas de protección

Los sistemas y aplicaciones de seguridad instalados no reemplazan el uso responsable y seguro de los dispositivos

ACCESO AL DISPOSITIVO

$4FtAm3!

Establecer un código de acceso al dispositivo

Para garantizar la seguridad de nuestros aparatos, ya se trate de ordenadores o de dispositivos móviles, se recomienda **proteger el acceso** a los mismos mediante un código o contraseña robusto asociado a la pantalla de bloqueo, así como un código PIN para desbloquear la tarjeta SIM en el caso de teléfonos móviles.

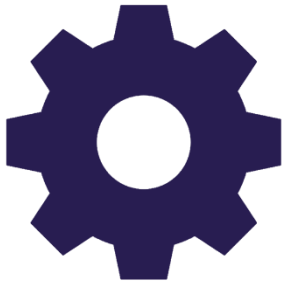
Teniendo en cuenta las implicaciones para la seguridad y la privacidad del contenido del dispositivo, se desaconseja utilizar métodos de acceso poco seguros como el deslizado de pantalla para desbloquear el aparato.

Los sistemas de protección de acceso más habituales son:

- **PIN**: código numérico. Se recomienda que contenga al menos 8 dígitos.
- **Patrón**: secuencia de movimientos sobre una matriz de puntos, donde se deben unir un mínimo de 4 de ellos. Se recomienda no utilizar patrones que se asemejen a letras del abecedario, así como desactivar la opción de mostrar el patrón dibujado.
- **Contraseña**: secuencia alfanumérica de hasta 16 caracteres. Es la opción de acceso más recomendable, utilizando una contraseña robusta de al menos 8 caracteres.

En su defecto, siempre que sea posible, se pueden utilizar sistemas biométricos de seguridad como el acceso con huella dactilar o el desbloqueo facial.

SISTEMA OPERATIVO



Mantener actualizado el sistema operativo de los dispositivos

Uno de los pilares de la seguridad de los dispositivos se encuentra en la eliminación de las vulnerabilidades de seguridad que puedan afectar a los mismos. Las brechas de seguridad más críticas suelen afectar al código bajo el que se desarrolla el sistema operativo.

Las actualizaciones periódicas ofrecidas por los desarrolladores contienen, entre otras cosas, correcciones de errores y los últimos **parches de seguridad**, especialmente aquellos de carácter crítico. Por ello, es recomendable comprobar de forma regular la existencia de dichas actualizaciones.

Es aconsejable **instalar estas actualizaciones de forma manual**, desactivando las opciones de actualización automática del sistema, y previamente realizar una copia de seguridad de los archivos que evite una posible pérdida de información.

APLICACIONES Y PROGRAMAS

Mantener actualizadas las aplicaciones y programas instalados en los dispositivos

La instalación de nuevos programas o aplicaciones puede afectar tanto al rendimiento como a la seguridad de los dispositivos.

Se recomienda comprobar frecuentemente la existencia de **actualizaciones** de las aplicaciones instaladas en el equipo, para protegernos frente a eventuales vulnerabilidades.

Instalar aplicaciones desde repositorios oficiales

Como medida de protección, es fundamental que instalemos las aplicaciones o programas únicamente desde **sitios de confianza**, para evitar suplantaciones que terminen en un problema de seguridad.

Los repositorios oficiales de aplicaciones son un lugar seguro desde el que instalarlas, ya que las aplicaciones pasan varios filtros de verificación de forma regular.

Google Play
Repositorio de aplicaciones Android

App Store
Repositorio de aplicaciones iOS

Microsoft Store
Repositorio de aplicaciones Windows

ARCHIVOS Y CARPETAS

Realizar copias de seguridad del contenido de los dispositivos

La protección de la información y los datos contenidos en los dispositivos debe ser considerada para evitar el riesgo de pérdida no deseada de datos ante el robo o desaparición del dispositivo.

Por ello, se deben realizar **copias de seguridad** periódicas y, si es posible, programadas de forma automática. Se recomienda realizar una copia en utilidades de almacenamiento en la nube, como Dropbox o Google Drive, y otra en un dispositivo físico sin conexión a Internet como memorias USB o discos externos.

El uso de copias de seguridad también reduce el daño que pueda ocasionar un ataque peligroso con previsible pérdida de información, como el que se produce mediante ransomware.

Los elementos más sensibles de los que se puede realizar copias de seguridad individuales son:

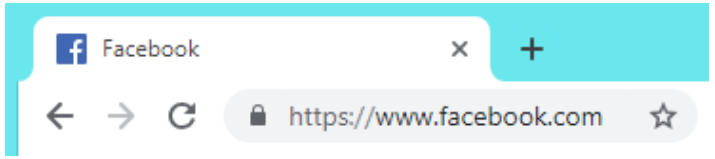
- Archivos y carpetas
- Contactos
- Fotos y vídeos
- Datos de aplicaciones
- Ajustes del sistema

NAVEGACIÓN WEB

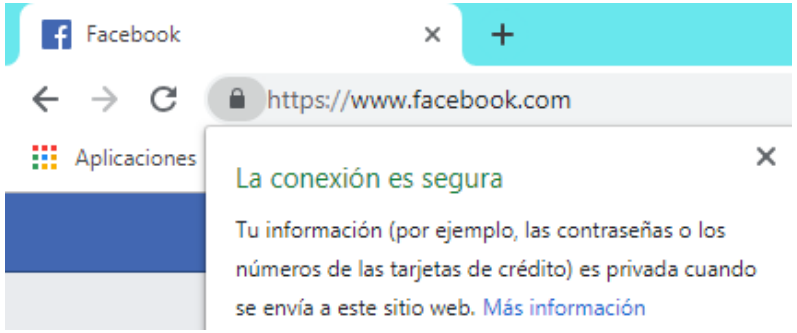
Elegir páginas web con navegación segura HTTPS://

Siempre que sea posible, se recomienda navegar por páginas que hayan implementado el Protocolo Seguro de Transferencia de Hipertexto o **HTTPS**. Este sistema incorpora un canal de cifrado basado a su vez en los protocolos conocido como SSL/TLS que garantiza la seguridad del tráfico de datos sensibles, fundamental si vamos a utilizar servicios de intercambio de información privada como correo electrónico, redes sociales o banca electrónica.

Para distinguirlo del protocolo HTTP, que no incorpora capa de seguridad, basta con consultar la barra de direcciones del navegador y observar que el inicio de la dirección URL sea https://. Como refuerzo visual todos los navegadores muestran un icono de candado cerrado que nos ayuda a saber que estamos navegando por un sitio seguro.



Además, se recomienda verificar a través del navegador el certificado de seguridad. Para ello basta con pulsar sobre el icono del candado y recibiremos la confirmación de estar ante un sitio seguro.



CONEXIONES INALÁMBRICAS

No conectar los dispositivos a redes WiFi públicas abiertas

Las redes Wifi públicas abiertas no requieren de una contraseña de acceso y nos facilitan una conexión rápida. Sin embargo, al conectarnos a una de estas redes estamos poniendo en riesgo la seguridad de nuestros dispositivos ya que el contenido que circula por las mismas no se cifra. Lo mismo puede suceder con redes con gran cantidad de usuarios conectados (bar, hotel, etc.) que pese a tener contraseña de acceso no podemos saber quién se conecta a ellas ni de qué modo se está transmitiendo la información.

En caso de necesitar conectarnos a unas de estas redes se recomienda:

- Evitar acceder con credenciales privadas a servicios que supongan una transmisión de datos sensibles como banca electrónica o comercio en línea.
- Pausar sincronizaciones de servicios de intercambio de datos o imágenes, como correo electrónico o servicios de almacenamiento en la nube.
- No memorizar los datos de la red pública para evitar que el dispositivo se vuelva a conectar en un futuro sin nuestro permiso.

Deshabilitar las conexiones inalámbricas (WiFi, Bluetooth, NFC…)

Para proteger los dispositivos de accesos remotos no deseados, se recomienda deshabilitar toda clase de conexiones inalámbricas tras su uso.
Se recomienda mantener únicamente activada la conexión de datos móviles, para permitir la localización del dispositivo en caso de pérdida.

GEOLOCALIZACIÓN

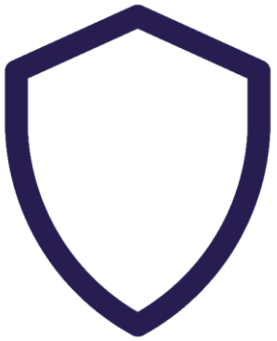
Deshabilitar los servicios de localización de los dispositivos

Uno de los datos privados más sensibles que los dispositivos recogen es el de la ubicación en tiempo real. La localización puede quedar expuesta a terceros, así como relacionarse con otros parámetros que permitan obtener información adicional que ponga en riesgo tanto la seguridad de los dispositivos como la personal.

La ubicación de un dispositivo puede ser rastreada con fines maliciosos mediante el módulo GPS del aparato, pero también a través de las redes WiFi, redes de fibra óptica o detectando la señal de telefonía móvil.

Por ello, se recomienda deshabilitar el uso de servicios de localización de todas aquellas aplicaciones, programas o página web cuyo cometido principal no tenga una funcionalidad expresa de ubicación, así como desactivar de forma específica el etiquetado de ubicación tanto en aplicaciones de fotografía como en redes sociales.

SISTEMAS DE PROTECCIÓN



Utilizar herramientas antivirus y antimalware

Para proteger los dispositivos frente a las **amenazas en línea** más generalizadas como es el malware o software malicioso, se recomienda contar con herramientas de protección específicas.

Cortafuegos o firewall	Herramienta que monitoriza las conexiones entrantes y salientes del dispositivo. Sirve para bloquear accesos no autorizados. Como norma general no se deben permitir conexiones de fuentes desconocidas.
Antivirus	Programa que nos protege del software malicioso detectando, deteniendo y eliminando posibles amenazas que aprovechan las vulnerabilidades de seguridad de los dispositivos. Los más completos incorporan en una única herramienta sistemas antimalware, antispyware y de eliminación de adware.

Es aconsejable mantener actualizadas de forma automática las herramientas de protección ante amenazas, ya que la naturaleza de las mismas cambia constantemente.

Se debe contar con medidas de protección independientemente del sistema operativo utilizado por el dispositivo

CANALES DE INFORMACIÓN

Mantenerse informado de las amenazas y riesgos actuales

Se crean nuevas ciberamenazas cada día, por lo que es recomendable estar informado a través de **canales oficiales especializados** para mantener la seguridad de nuestros dispositivos y obtener formación en ciberseguridad.

OSI Oficina de Seguridad del Internauta

Centro Criptológico Nacional
https://www.ccn-cert.cni.es/

CCN-CERT centro criptológico nacional

Centro Criptológico Nacional
https://www.ccn-cert.cni.es/

ASOCIACIÓN DE INTERNAUTAS

Asociación de Internautas
https://www.internautas.org/

enisa

Agencia Europea de Seguridad de las Redes y de la Información (ENISA).
https://www.enisa.europa.eu/

SENTIDO COMÚN

- Establecer un código de acceso al dispositivo
- Mantener actualizado el sistema operativo de los dispositivos
- Mantener actualizadas las aplicaciones y programas instalados
- Instalar aplicaciones desde repositorios oficiales
- Realizar copias de seguridad del contenido de los dispositivos
- Elegir páginas web con navegación segura HTTPS://
- No conectar los dispositivos a redes WiFi públicas abiertas
- Deshabilitar las conexiones inalámbricas (WiFi, Bluetooth, NFC…)
- Deshabilitar los servicios de localización de los dispositivos
- Utilizar herramientas antivirus y antimalware
- Mantenerse informado de las amenazas y riesgos actuales

PARA SABER MÁS...

[a personalizar por cada institución]

¡Si tienes dudas pregunta a los bibliotecarios!

CRUE REBIUN
Red de Bibliotecas Universitarias