USO PRÁCTICO DEL SMARTPHONE, TABLET E INTERNET. AVANZADO

TEMA 2

ANTONIO FERNÁNDEZ HERRUZO

Privacidad en una Web

- Las empresas cada vez manejan más y más datos de clientes en internet.
- Deben cumplir con la ley de protección de datos. RGPD
- La política de privacidad se creó con la finalidad de proteger y preservar los derechos del espacio privado de las personas. **Cada vez que entramos en un sitio web y nos registramos como usuarios,** estamos facilitando nuestros datos personales a la empresa. Con ella lo que conseguimos es que se establezcan unos límites para el uso de estos datos e información.
- Por tanto, esta política dicta como debe ser utilizada y almacenada dicha información.

Privacidad en una Web

- Siempre que se dan datos en una app o web se deben Aceptar la Política de Privacidad de la empresa.

- La dura verdad es que hoy en día **(casi) nadie se lee los términos de uso ni la política de privacidad de los servicios que usa**, y a la mayoría sólo les importa cuando se genera alguna polémica y sale a la luz.

- Distintos modelos de recogida de datos. Enlace

Privacidad en una Web

PÁGINAS WEB

Política de cookies

Una cookie es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

Aviso Legal

Texto donde se informa a los usuarios sobre quién es el propietario de la página web.

Política de Privacidad

Texto donde se informa al usuario de la página web sobre cómo van a tratarse sus datos personales.

Condiciones Generales de Contratación

Conjunto de cláusulas que regulan la forma en la que los usuarios realizan pedidos o solicitudes de compra en la página web y los derechos, obligaciones y responsabilidades que corresponden a cada parte.

Modelo de solicitud para requerir el consentimiento en todos los formularios (contacto, suscripción)

El RGPD exige un consentimiento expreso para poder tratar los datos personales. Por eso es necesario incluir un check desmarcado por defecto en todos los formularios online para aceptar la Política de privacidad.

Privacidad en una App

APP MÓVILES

Política de privacidad APP

Texto donde se informa al usuario de la aplicación móvil sobre cómo van a tratarse sus datos personales.

Condiciones de uso APP

Documento que contiene el contrato entre la empresa y el usuario para la venta de productos o servicios.

Privacidad en una Web

BRECHAS DE SEGURIDAD

Notificación brecha de seguridad a la AEPD y a los afectados

Nueva obligación para Responsables del tratamiento de notificar las brechas de seguridad en 72 horas a la AEPD y a los titulares de esos datos.

Aviso Legal

- El aviso legal es el documento dentro de un sitio web que identifica a su propietario.
- Este documento debe tener entre otros los siguiente datos: (nombre, dirección, CIF/NIF, email, etc.)
- Debe estar en un sitio visible y desde cualquier página de la web.
- Normalmente se sitúan en el pie e la página.
- Ejemplo de una tienda online

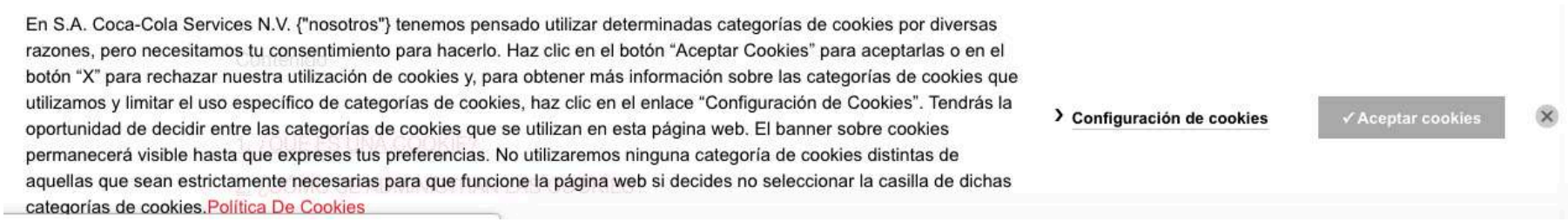
Política de Cookies

- Las cookies son **fragmentos de información enviados por un sitio web y almacenados en el navegador del usuario** que visita ese sitio.
- Gracias a ellas **se puede hacer un seguimiento del usuario** no sólo en el mismo sitio, sino en múltiples web (¿Te has fijado que has estado viendo un producto en una tienda online y luego te pasas 2 semanas viendo ese producto en todas las webs que visitas? Ahí están las cookies).

- Las cookies son necesarias para, por ejemplo, **seguir el proceso de una compra online**, pero también para cosas no tan necesarias aunque comunes como analizar las visitas a nuestra página web (ya sea con **Google Analytics**) o mostrar **publicidad dinámica**.

Política de Cookies

- En la mayoría de los casos, pueden ser de gran ayuda para mejorar nuestra experiencia en internet, creando un perfil de usuario y evitando que tengamos que rellenar formularios, contraseñas e interminables hojas de contacto una y otra vez.



Borrar Historial de Navegación

- "Si vacías la caché y eliminas las cookies de tu navegador, **se borrará la configuración de sitios web** (como los nombres de usuario y las contraseñas) y es posible que algunos sitios funcionen más lentamente, dado que todas las imágenes deben cargarse de nuevo".

- "Tendrás que volver a escribir los nombres de usuario y contraseñas, pero **tu privacidad estará más a salvo y tu navegador trabajará mejor**".
- En Google Chrome -> Configuración->Privacidad-> Borrar Historial
- En Ajustes-> Safari-> **Borrar historial** y datos de sitios web

Privacidad en una App

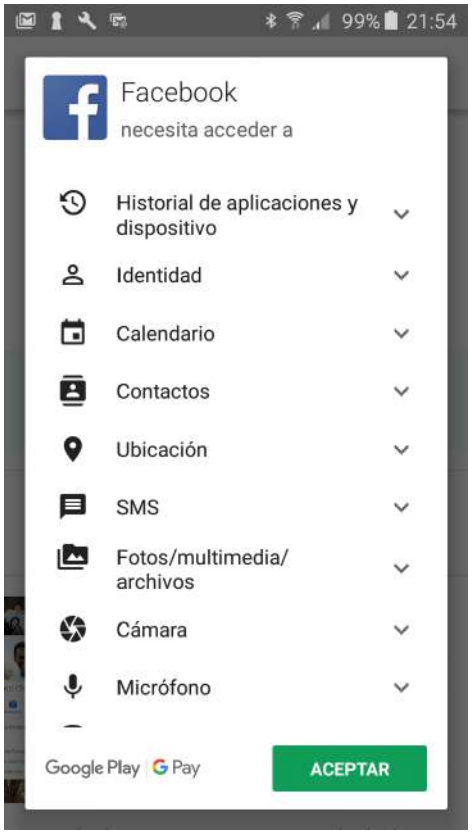
Clases de Aplicaciones móviles según los medios externos a los que entran:

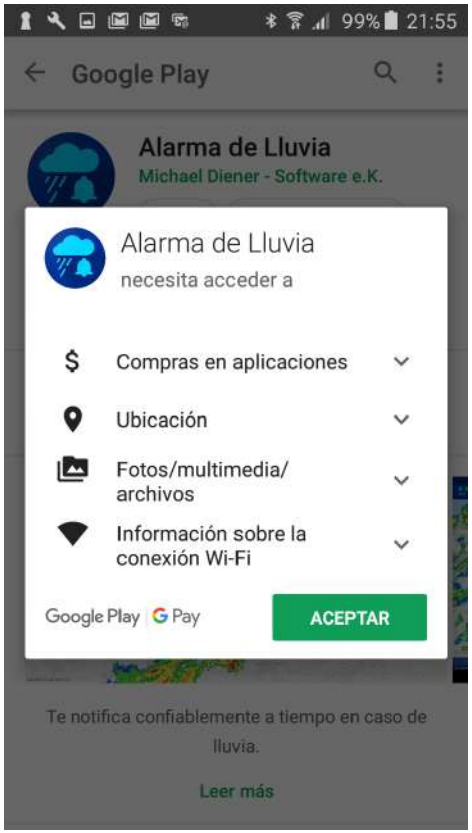
- **Apps "online"**: Serían aquellas apps que acceden a recursos online o a distancia. Entre ellas están las apps de noticias, mapas, consultas bancarias y especializadas, juegos y redes sociales, foros, apuestas, aviso de radares, ubicación geográfica, etc.
- **Apps "offline"**: Serían aquellas apps que no necesitan recursos online ni a distancia. Como por ejemplo determinados juegos que no acceden a redes de datos, ciertas aplicaciones de información, algunas herramientas ofimáticas, etc.

Según los medios internos a los que acceden:

- **Apps "invasivas"**: Serían aquellas que acceden a la agenda del dispositivo, al número de identificación del terminal, a su localización geográfica, a las fotos acumuladas, o exhiben publicidad, o falsifican el perfil del usuario en una red social determinada, o incluso las que exigen que el usuario se registre suministrando sus datos personales.
- **Apps "no invasivas"**: aquellas apps que no entran en ningún recurso interno o confidencial del dispositivo, ni exigen ningún dato personal del usuario.

Privacidad en una App





No hay nada gratis

¿Tu eres? ¿Dónde tu estas?

Permisos en las App

- Permisos para acceder a tu localización y tus cuentas.
- Con estos permisos la app puede acceder a quién eres y donde estas.
- La mayoría de app son gratuitas y estamos pagando con nuestra privacidad la app.
- Si se lo damos a una app como por ejemplo Facebook debemos saber que quieren darnos una experiencia personalizada para sus anuncios. De esta forma Facebook vende más cara la publicidad a sus anunciantes.

Permitir Localización

- Los sistemas operativos Android e iOS saben donde estamos (entre otros sistemas) por los mapas de redes WIFI. **NO NECESITAN TENER EL GPS ACTIVADO**. Si una persona accede a una red wifi y da su localización GPS, ya no necesita que tú tenga activado el GPS para saber donde estás.

- De esta forma lo saben 100% siempre donde estamos.

- Lo saben los sistemas operativos y la compañías de teléfono.

- La ubicación dice donde vives, donde trabajas, donde compras, si vas andando, si vas en bici o en coche, si eres rico o pobre, a quién visitas…

Compra de Datos

- Es una situación muy común. Recibes, sin saber muy bien desde dónde, publicidad que nunca has pedido que te envíen. Un mensaje de texto, una llamada de teléfono ofreciendo un producto a unas horas intempestivas o un bombardeo de correos electrónicos que con mayor o menor fortuna tu filtro de *antispam* puede bloquear. Tus datos están ahí fuera y alguien se está lucrando con ellos.

- Empresas de marketing usan bases de datos con información personal de miles de personas. Cientos de miles en casos de grandes campañas. En ellas se encuentran nombres y apellidos, números de teléfono -fijo y/o móvil-, correos electrónicos y direcciones físicas. Incluso se puede clasificar a las personas dependiendo de sus gustos.

No todo es malo…

- Si alguien utiliza tu tarjeta de crédito en una ubicación donde no estés en el momento actual. ¿Será probable que te hayan robado la tarjeta? Los sistemas antifraude utilizan estos métodos y muchos más.
- Servicios de tráfico para que avisen de la ruta más corta en el momento actual (servicios como Waze) o atascos y carreteras cortadas.
- Saber donde hay probabilidad de enfermedades.
- Predecir los planes de emergencia.
- Perfiles para mejorar la experiencia en compras.
- Publicidad dirigida y personalizada.

Para reflexionar

Tenemos que pensar si ese servicio que me prestan merece la pena que lo pague con mis datos.

Seguridad ¿nos importa?

- La gran mayoría de los servicios y sistemas que utilizamos en el día a día requieren como único control de acceso un nombre de usuario y contraseña. En estos casos, la clave actúa como una llave digital que le permite a un usuario identificarse en el sistema para poder acceder a información sensible. De este modo, dicha contraseña protege los datos privados del acceso no autorizado por parte de terceros.

- Sin embargo, el aumento de ataques informáticos sumado a las conductas inseguras de las personas, como las contraseñas débiles e iguales en varios servicios, hacen necesario utilizar otros métodos de autenticación más robustos. Por lo mismo, muchas empresas están implementando la doble autenticación.

Desbloqueo del SmartPhone

- La seguridad de los datos que están en nuestros Smartphone es algo a lo que le damos (o deberíamos de darle) mucha importancia, sobre todo en aquellos casos en los que guardamos información sensible (contraseñas, cuentas bancarias...)

- Con la llegada y extensión masiva del sensor de huellas (pocos son los modelos que prescinden de él a día de hoy), ya casi nos olvidamos de teclear el PIN, la contraseña o de **deslizar el dedo para usar el patrón**.

- Es muy importante tener algún sistema de los mencionados en nuestro teléfono.

Ataque informáticos

- **Fuerza bruta**: software que utiliza un diccionario para descifrar contraseñas combinando distintos caracteres y palabras de forma aleatoria.
- **Phishing**: falsificación de una entidad de confianza como bancos o redes sociales por parte de un cibercriminal. De este modo, el atacante busca manipular a la víctima para que ingrese sus credenciales de acceso en un sitio fraudulento.
- **Malware**: programa diseñado para realizar diversas acciones maliciosas, como el robo de contraseñas y credenciales de acceso.
- **Ataques a servidores**: vulneración de un sistema informático utilizado para almacenar la base de datos de credenciales de acceso de un determinado servicio.

Mucho cuidado con los Correos Fraudulentos

- Siempre tener cuidado al abrir correos electrónicos de remitentes desconocidos con documentos adjuntos.
- Siempre tener cuidado al hacer clic en enlaces incluidos en correos electrónicos de remitentes desconocidos
- Instalar aplicaciones antimalware y activar los filtros antispam
- Usar siempre contraseñas seguras
- **Evitar utilizar el correo electrónico desde conexiones públicas**
- Cifra el correo electrónico al enviar información confidencial
- No publicar direcciones de correo electrónico en la web de la empresa ni en sus redes sociales
- Nunca responder al correo basura
- Desactivar el HTML en las cuentas de correo críticas
- Utilizar la copia oculta (BCC o CCO) cuando se envíen direcciones a múltiples destinatarios

Redes Públicas

- Las wifis públicas son aquellas que no están protegidas por una contraseña y nos permiten conectarnos a Internet de una forma cómoda y rápida. Estas redes no cifran la información que se transmite a través de ellas.

- Video como espiar a alguien en un red wifi: https://www.youtube.com/watch?v=hpF7LhMXu5I

Sistemas de Doble Autentificación

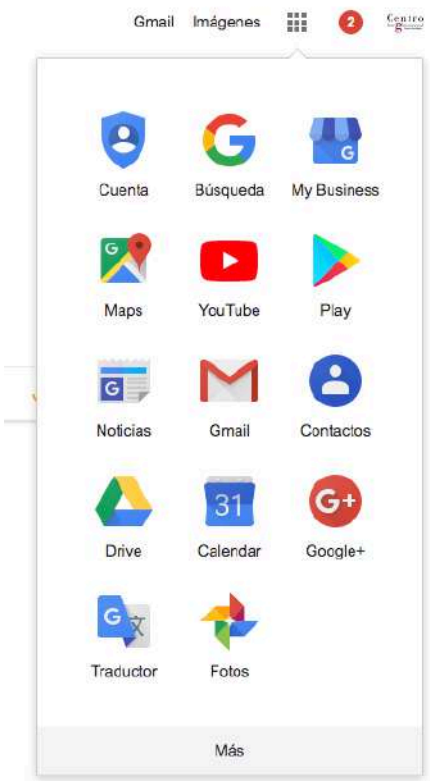
- Un sistema de doble autenticación es aquel que utiliza dos de los tres factores de comprobación para validar al usuario. Estos factores pueden ser:
- Algo que el usuario sabe (conocimiento), como una contraseña.
- Algo que el usuario tiene (posesión), como un teléfono o token que le permite recibir un código de seguridad.
- Algo que el usuario es (inherencia), o sea, una característica intrínseca del ser humano como huellas dactilares, iris, etc.
- Por motivos económicos y de factibilidad, los sistemas de doble autenticación suelen utilizar los factores conocimiento (nombre de usuario y contraseña) y posesión (teléfono o token para recibir código de seguridad) en detrimento del factor inherencia o sistemas de biometría.

iPad robado de Steve Jobs

- **Un payaso profesional tenía el iPad robado en la casa de Steve Jobs**

- Los investigadores de Apple identificaron a McFarlin después de que utilizó su cuenta de iTunes para conectarse a Internet desde los dispositivos robados, dijo la Policía.

Mi cuenta de Google

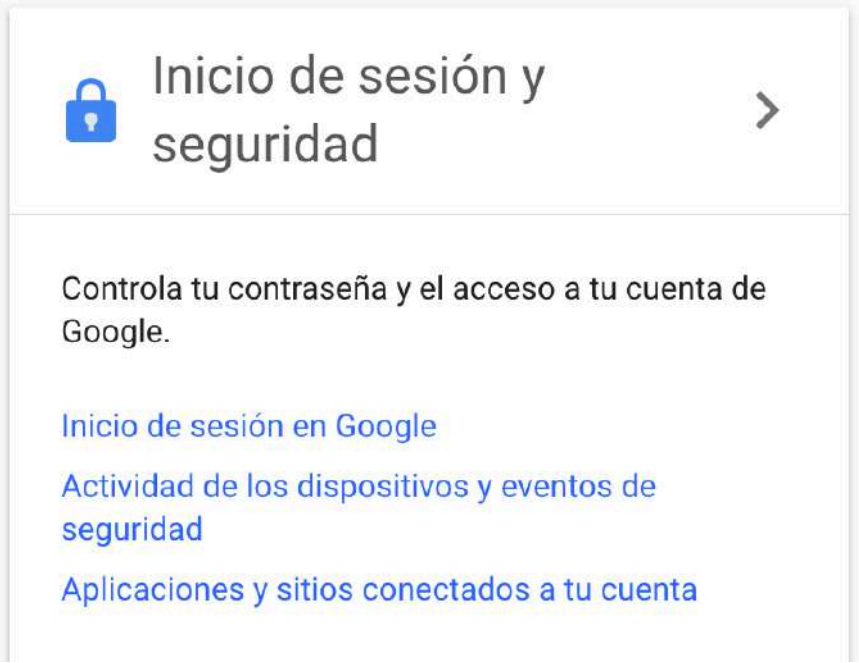


Privacidad de Google

- Desde Mi Cuenta puedes acceder a herramientas para proteger tu datos y tu privacidad, y decidir cómo quieres que tu información contribuya a mejorar el funcionamiento de las herramientas y los servicios de Google.
- Revisa las actividades recientes relacionadas con el dispositivo y la seguridad en tu cuenta.
- Puedes cambiar los datos de tu cuenta, teléfono, correo electrónico de recuperación
- Preferencias del sistema, capacidad de Google Drive.
- Eliminar los datos de tu cuenta.

Aplicaciones y sitios conectados a tu cuenta

- Las contraseñas que usas en Chrome y en Android se guardan con Google Smart Lock y se recuerdan en todos los dispositivos en los que hayas iniciado sesión.



Mi actividad

- Los datos que guardan en tu cuenta pueden hacer que servicios de Google te sean mucho más útiles y recibas, por ejemplo, más opciones de transporte público en Maps o resultados más rápidos en el buscador.