GESTIONES DIGITALES CON LA ADMINISTRACIÓN

13 de ENERO de 2026, 10 am – 13 am

“Proyecto Comunidad Digital ATC-Las Rozas”

AMERICAN TOWER
ESPAÑA

Las Rozas

comunidades digitales

Contraseña Portatil: Cantizal.2025
Wifi WLR_Cantizal
Usuario: cantizal
Contraseña: Cantizal01

"Proyecto Comunidad Digital ATC-Las Rozas"

AMERICAN TOWER
ESPAÑA

Las Rozas

comunidades digitales

Adecco
Learning & Consulting

LAS ROZAS
SMART CITY

Gestiones Digitales con la Administración

¡Bienvenidos al curso de Introducción a los Gestiones Digitales con la Administración!

Me llamo Mariano, formador homologado de Adecco, y durante las próximas 3 horas aprenderemos juntos cómo realizar gestiones administrativas desde casa usando ordenadores o dispositivos móviles. Y a protegernos al hacerlo.

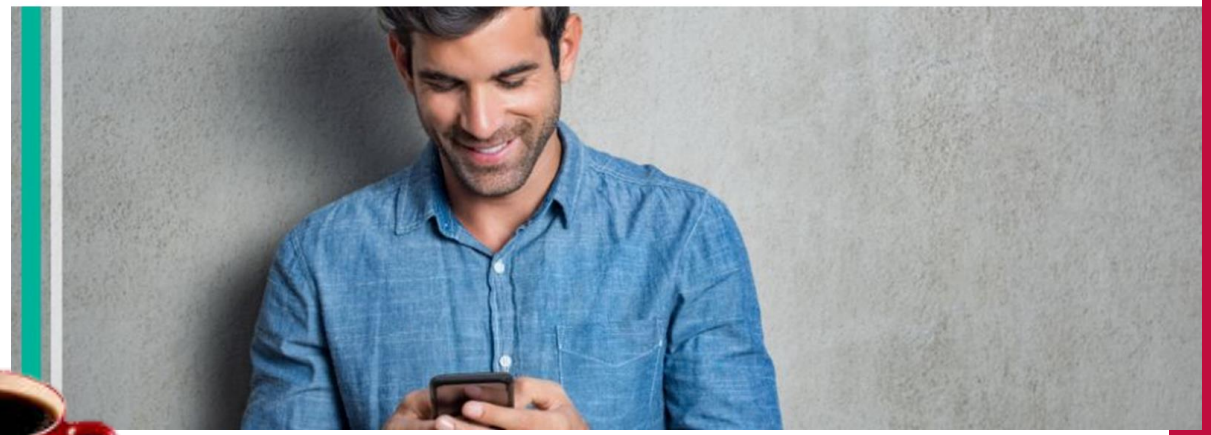
Este curso está especialmente diseñado para personas que desean iniciarse en el uso de internet para gestiones cotidianas, aunque no tengan mucha experiencia previa con la tecnología.

.

Manejo Eficiente de Certificados Electrónicos

Certificado Digital, Clave y DNI

Administración electrónica



Pagos Digitales y Gestión Financiera Online

Ciberseguridad para Principiantes

Manejo Eficiente de Certificados Electrónicos

Certificado Digital, Clave y DNI

Certificado digital, Cl@ve y DNI digital, ¿qué son?

- **Certificado digital**: Permite verificar la identidad de una persona o una entidad en el ámbito digital.

- **Cl@ve**: Sistema de identificación electrónica que facilita el acceso a servicios públicos a través de Internet.

- **DNI digital**: Es una versión electrónica del documento nacional de identidad.

Adecco
Learning & Consulting

Identificación mediante certificados digitales

¿Qué es un **certificado digital**?

Es un **archivo informático** que permite **autenticar** la identidad de una persona, empresa o entidad en Internet.

Es emitido por una autoridad de certificación reconocida y funciona como un "**carnet de identidad digital**".

Contiene información clave como el **nombre del titular**, una **clave pública** y la **firma de la autoridad emisora** que garantiza su validez.

Adecco
Learning & Consulting

Cómo funciona un certificado digital

El funcionamiento de los certificados digitales se basa en la **criptografía** (algoritmos codificados que protegen y ocultan la información transmitida) de clave pública.

Este método emplea un par de claves:

- **Clave privada**: Es secreta y está bajo el control exclusivo del usuario. Permite **firmar documentos** electrónicos o **autenticar** su identidad.

- **Clave pública**: Es accesible a cualquier tercero y está incluida en el certificado digital. Sirve para **verificar la firma digital** generada por la clave privada.

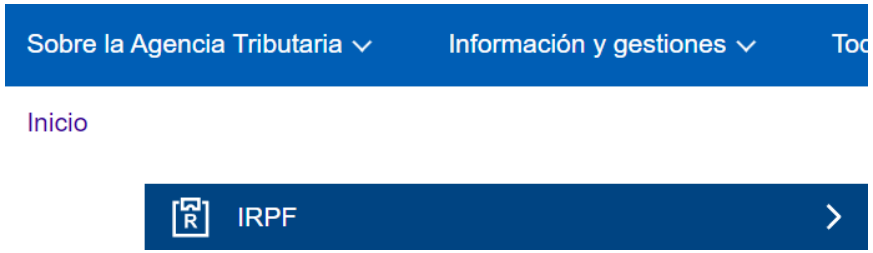
Adecco
Learning & Consulting

Ejemplo práctico de funcionamiento

Acceso al portal de la Agencia Tributaria para la presentación del Impuesto sobre la Renta:

1

2



3

4

Dónde se usan los certificados digitales

- **Acceso a portales oficiales**
- **Firma electrónica de documentos**
- **Gestión empresarial** (impuestos, liquidaciones)
- **Seguridad en transacciones en línea** (compras on line, transferencias bancarias)
- **Cifrado de comunicaciones corporativas**

Adecco
Learning & Consulting

Ventajas de los certificados digitales

- Seguridad y reducción de riesgos
- Validez legal de las firmas electrónicas
- Ahorro de tiempo y recursos
- Comodidad y accesibilidad
- Compatibilidad con múltiples servicios

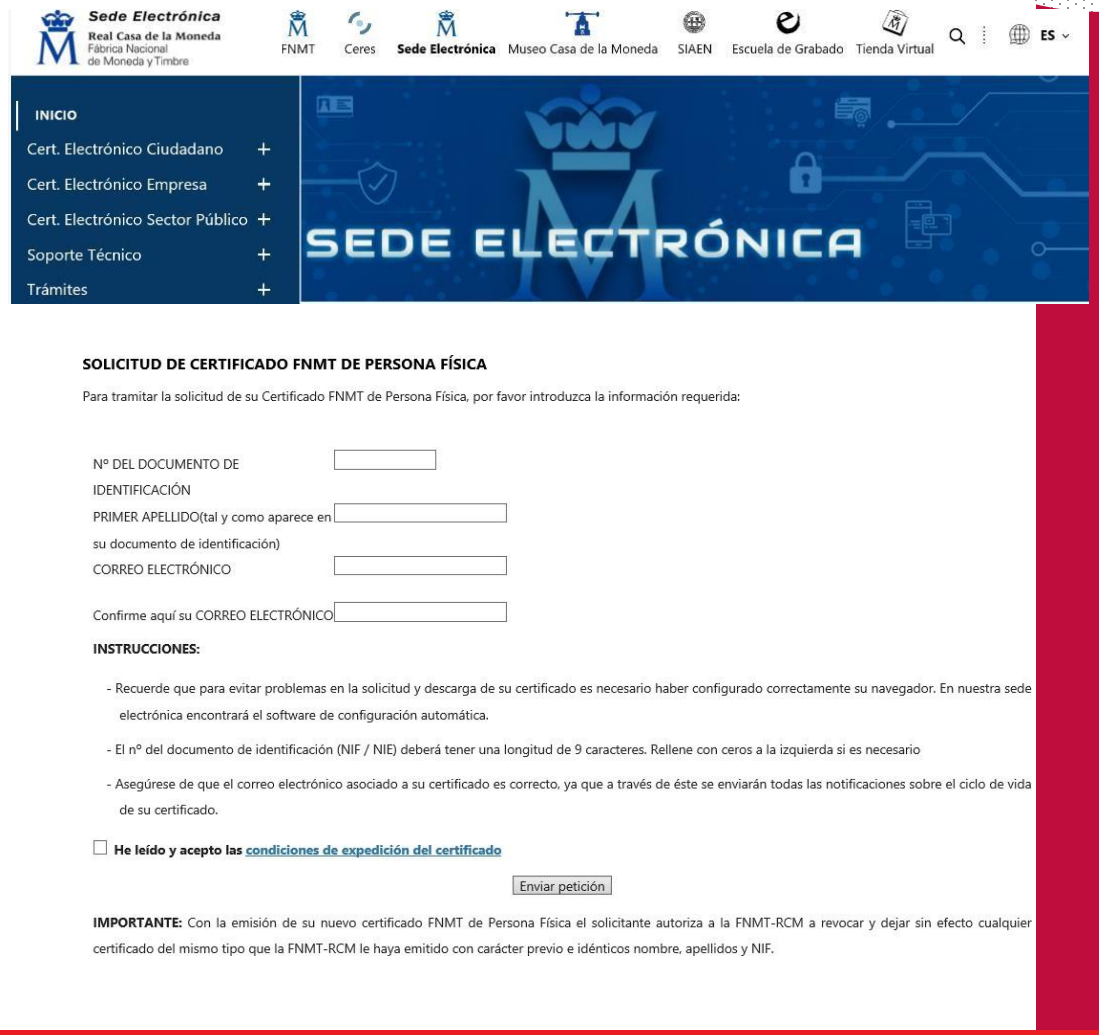
Comparativa de los certificados digitales

	CERTIFICADO DIGITAL	DNIe	CL@VE
EMISIÓN	Autoridad de Certificación (FNMT, etc.).	Dirección General de la Policía.	Sistema Cl@ve.
OBTENCIÓN	Procedimiento complejo: requiere personación física.	Inmediata.	Depende del procedimiento elegido: Internet, personación física o vía postal.
USO PRINCIPAL	Autenticación del usuario y la firma digital de documentos.	Autenticación del usuario y la firma digital de documentos.	Autenticación del usuario y la firma digital de documentos.
ORGANISMOS COMPETENTES	Administración Central, Autonómica y Local, junto a empresas del ámbito privado.	Administración Central, Autonómica y Local, junto a empresas del ámbito privado.	Organismos del Sector Público.
VALIDEZ	Depende del tipo de CA y de certificado, sin superar los 60 meses.	60 meses.	En función del tipo de Cl@ve abarca desde la duración del trámite, hasta los 24 meses.
INCONVENIENTES	Dificultad para tramitación y problemas con navegadores web obsoletos.	Se necesita un lector de tarjetas adicional para su uso.	Sin disponer de certificado digital o DNIe el proceso de obtención se dilata.
VENTAJAS	De uso común en ámbito empresarial, es el mecanismo más seguro y ágil.	Al estar incorporado en el DNI siempre se lleva encima.	Facilidad de uso e instantaneidad para trámites sencillos.

Adecco
Learning & Consulting

Cómo adquirir un certificado digital

1. Elegir la entidad emisora (FNMT, Camerfirma, GlobalSign...)
2. Acceso al portal de la entidad emisora (p. ej., FNMT)
3. Generar la solicitud del certificado:
    1. Descarga e instalación del software requerido
    2. Proporcionar datos personales y correo electrónico
4. Verificación de identidad
    1. Código de verificación + DNI (pasaporte o carné de identidad)
    2. En persona o electrónicamente



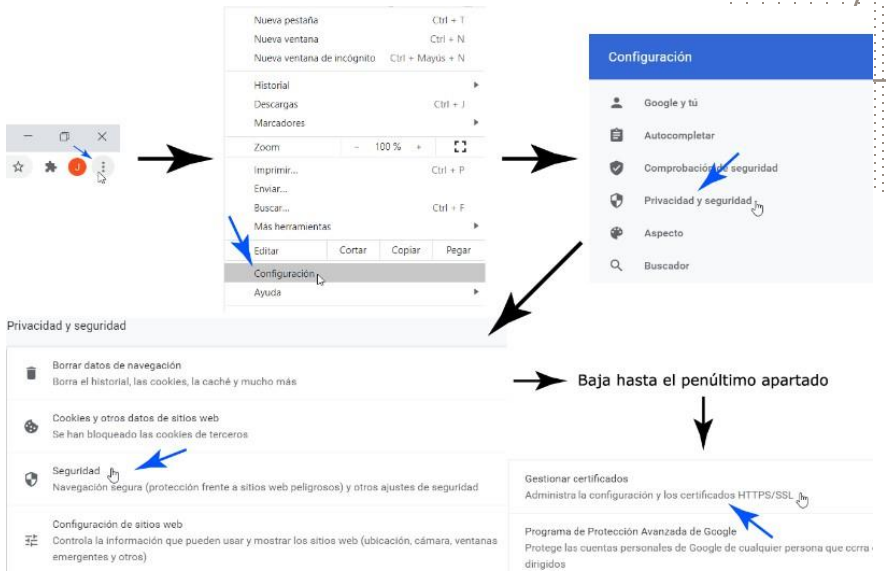
Descarga del certificado digital

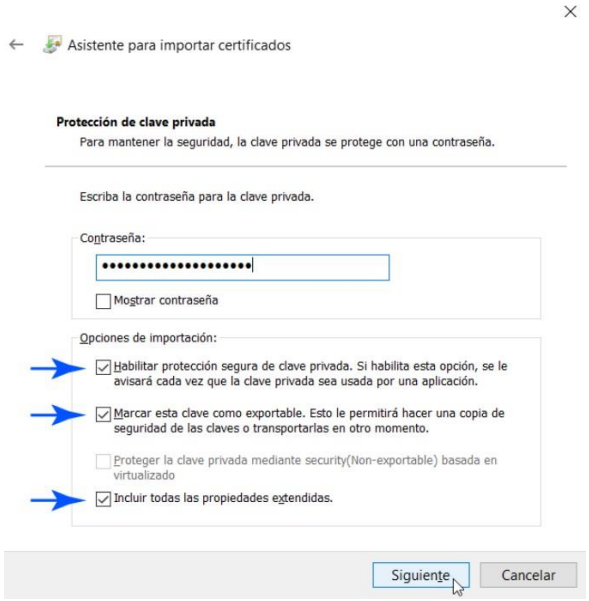
1. **Acceso al portal de descarga**
2. **Introducción de datos + código de verificación**
3. **Verificación de clave privada**
4. **Exportación del certificado** (opcional)

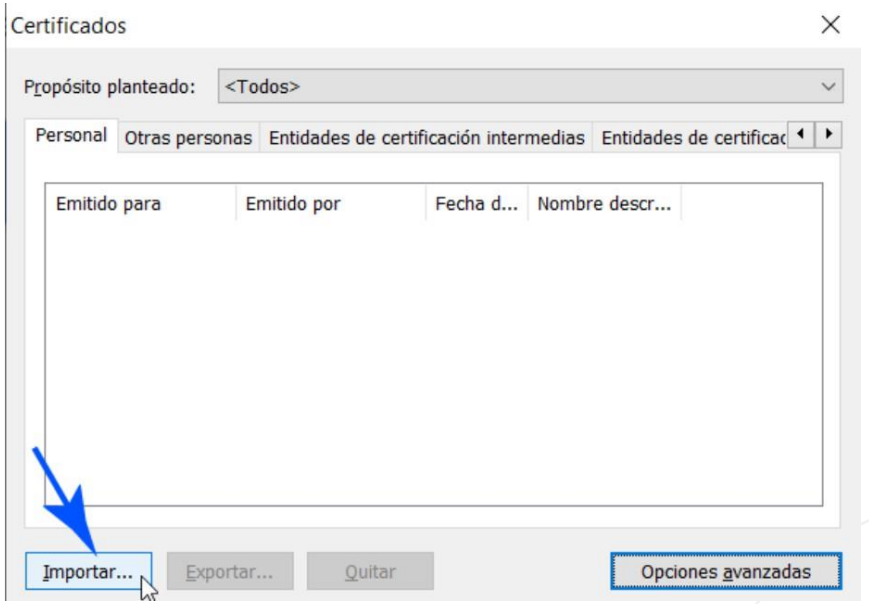
Instalación del certificado digital

Navegadores

1. Configuración > Seguridad > Importar certificado
2. Ingreso de contraseña del archivo exportado







Qué es el sistema Cl@ve

- Sistema para identificarte electrónicamente en las gestiones con las Administraciones Públicas.
- Unifica y simplifica el acceso electrónico a los servicios públicos.
- Plataforma común para la identificación, autenticación y firma electronica.
- Requiere registro previo, que puede ser:
  - Presencial en oficina adherida al sistema
  - Online, utilizando un certificado electrónico
- El registro proporciona 2 tipos de clave de acceso:
  - Cl@ve PIN
  - Cl@ve permanente

Cl@ve PIN

- Forma de realizar trámites por Internet con una validez limitada en el tiempo.
- Permite acceso seguro a servicios públicos.
- Se puede renovar cada vez que necesitemos.
- Requiere registro previo en el sistema Cl@ve.

Ventajas:

- Es muy sencillo. No es necesario recordar una contraseña de forma permanente.
- Validez limitada en el tiempo. Otorga seguridad.

Funcionamiento de Cl@ve PIN

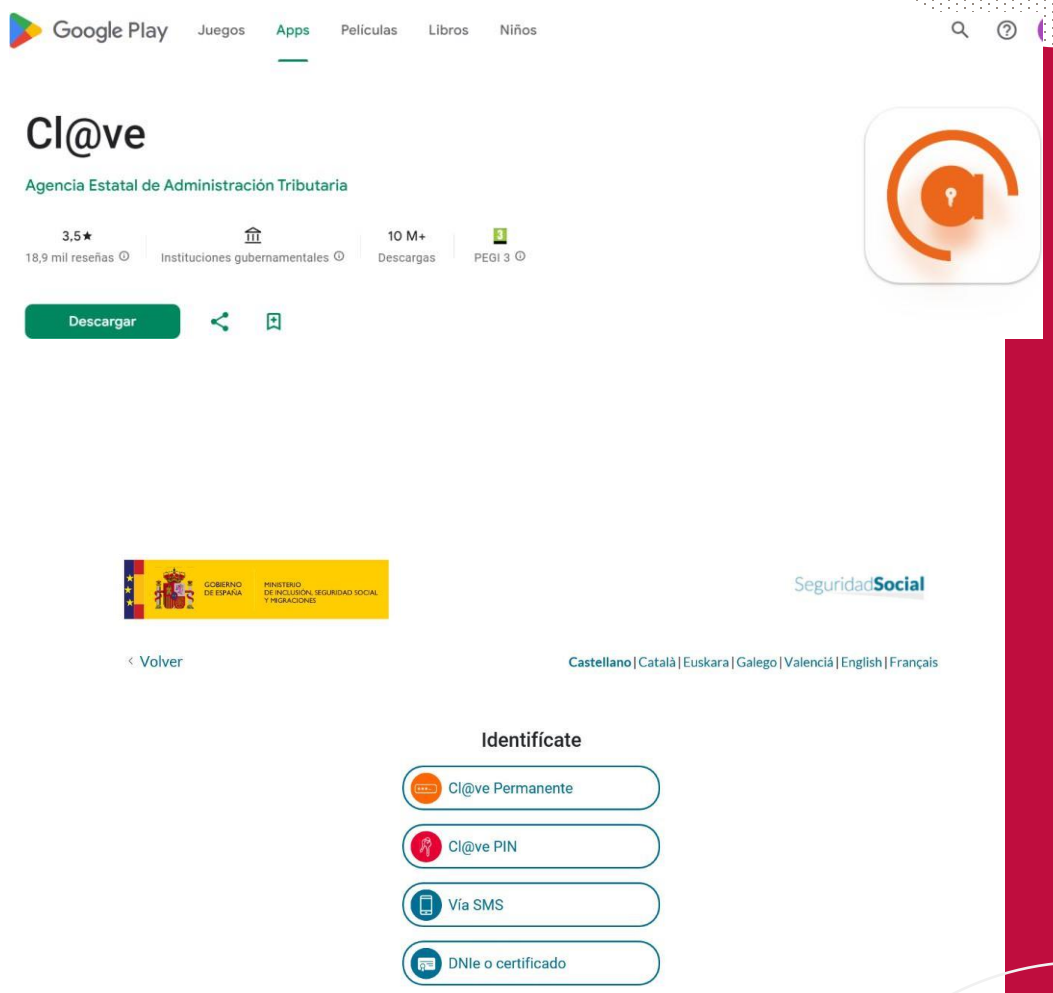
1. Una vez registrados, se obtiene una Cl@ve PIN para acceder a los trámites.

2. Por seguridad, el PIN sólo puede ser utilizado una vez.

3. Podemos obtener el PIN de dos formas:
   - Obtención Cl@ve PIN mediante app móvil (recomendado)
   - Obtención Cl@ve PIN mediante SMS

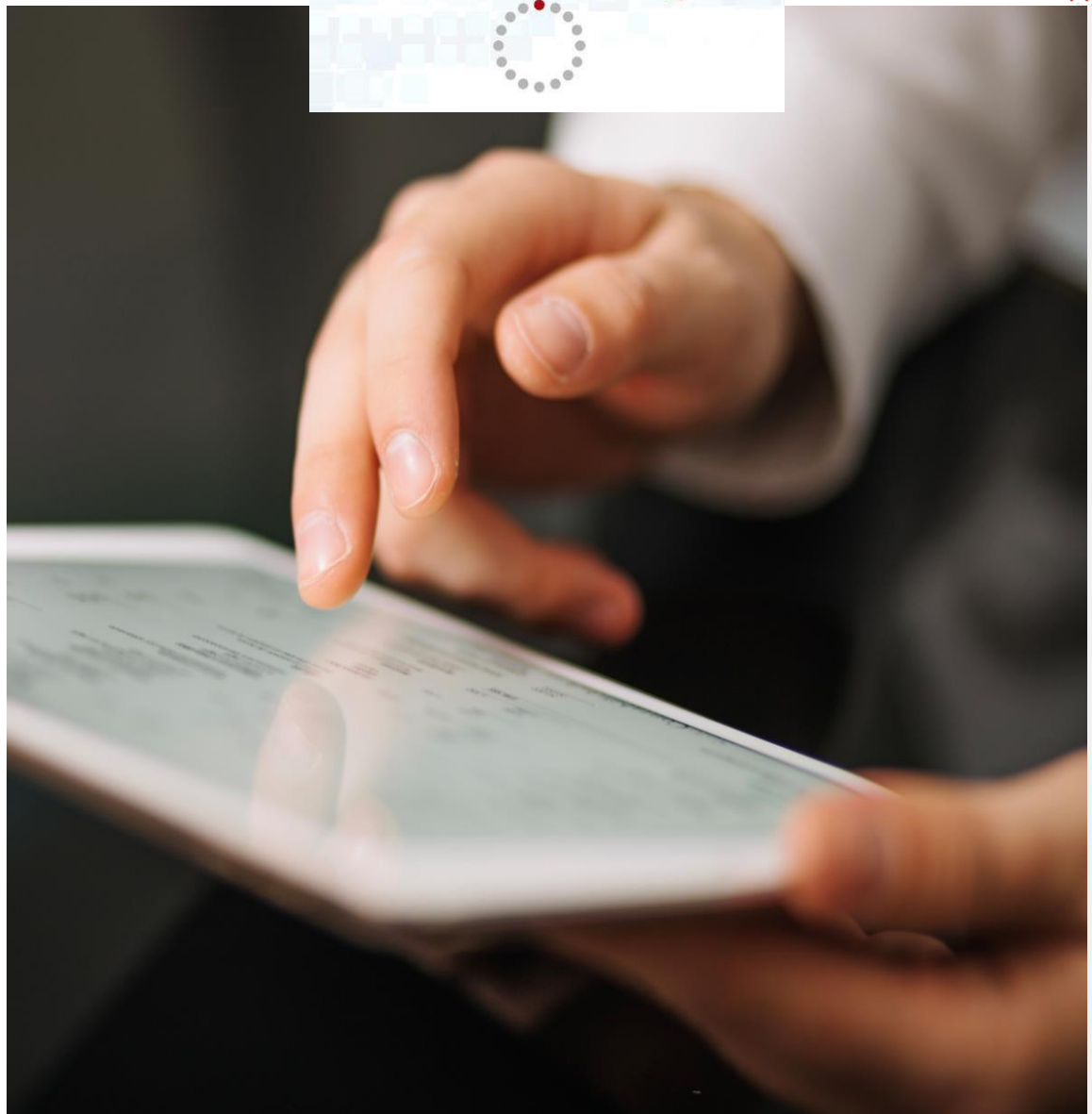
1. El PIN recibido tiene validez durante 10 minutos. Pasado ese tiempo, debemos solicitar otro PIN.

4. La identificación mediante el PIN permite acceder mientras no nos desconectemos de la Sede Electrónica o cerremos el navegador.



Qué es AutoFirma

- Aplicación de firma electrónica desarrollada por el Ministerio de Asuntos Económicos y Transformación Digital.
- Permite la firma en documentos dentro de un procedimiento administrativo de forma sencilla.
- Requiere tener un certificado electrónico instalado para poder utilizarla.
- Una vez instalada, permanece en nuestro dispositivo hasta que se decida desinstalarla.



Funcionamiento de AutoFirma

- Requisitos previos:
  - Certificado digital instalado en el equipo.
  - Descarga de AutoFirma desde su web oficial
- Pasos generales para usar AutoFirma:
  - Abrir un documento.
  - Seleccionar el certificado.
  - Firmar y guardar el archivo.

Descargas

Desde aquí puedes descargarte aquellas aplicaciones que necesites para firmar electrónicamente y otras utilidades o documentos.

AutoFirma

autofirm@

Aplicación de firma electrónica desarrollada por el Ministerio de Asuntos Económicos y Transformación Digital. Al poder ser ejecutada desde el navegador, permite la firma en páginas de Administración Electrónica cuando se requiere la firma en un procedimiento administrativo.

- AutoFirma 1.8.3 para Windows 64 bits
- AutoFirma 1.8.3 para Windows 32 bits
- AutoFirma 1.8.3 para Debian Linux
- AutoFirma 1.8.3 para Fedora Linux
- AutoFirma 1.8.3 para OpenSUSE Linux
- AutoFirma 1.8.4 para MacOS procesadores x64

Adecco
Learning & Consulting

Conclusión

Comparativa de sistemas:

- Cl@ve PIN: identificación rápida para acceder a servicios online.
- AutoFirma: validez jurídica en documentos electrónicos.

Beneficios:

- Simplificación de trámites.
- Mayor seguridad en gestiones digitales.

Páginas de interés

Fábrica Nacional de Moneda y Timbre (FNMT)

Información sobre el DNIe

Portal Cl@ve

Consulta y descarga de información de portales de la Administración

- Principales portales:
  - Agencia Tributaria: Consultas fiscales
  - Seguridad Social: Informes laborales, certificados de pensiones
  - SEPE: Prestación por desempleo
  - Otros: Sede electrónica de Ayuntamientos

- Proceso básico:
  - Accede a la página oficial
  - Identifícate con tu certificado o DNIe
  - Consulta o descarga el documento necesario

PORTAL → **IDENTIFICACIÓN** → **DESCARGA**

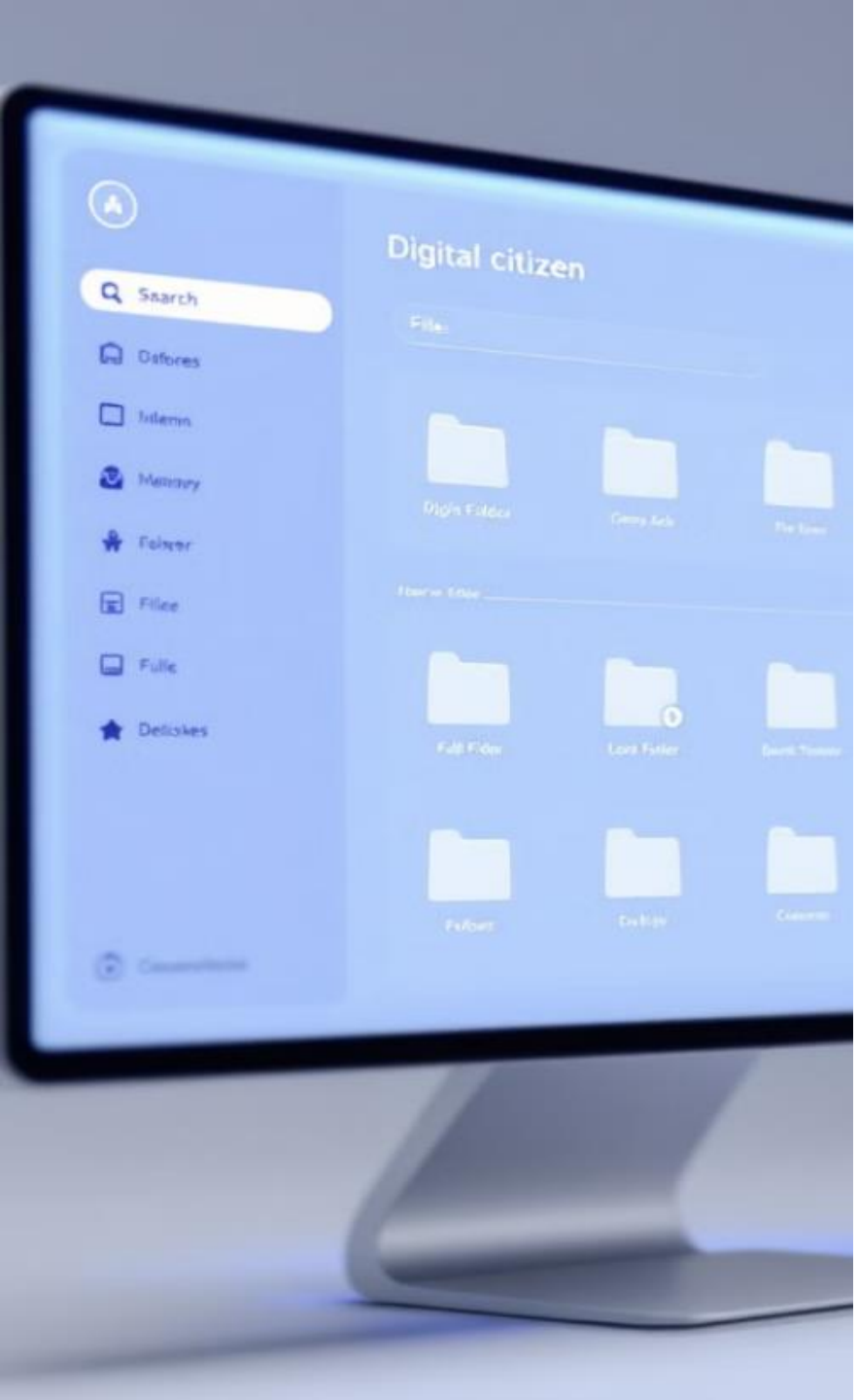
Conclusión

- Los certificados electrónicos y el DNIe son herramientas clave para la **gestión digital segura**.
- Siguiendo los pasos, cualquier usuario puede **instalarlos y utilizarlos** sin complicaciones.
- La tecnología facilita el acceso a servicios y **mejora la eficiencia** en trámites.

Administración electrónica

Modernización Digital en España: Servicios Electrónicos para Ciudadanos

Exploraremos las herramientas digitales que están transformando la interacción entre ciudadanos y administraciones públicas en España, mejorando la eficiencia y accesibilidad de los servicios gubernamentales.



La Carpeta Ciudadana

Gestión personalizada

Permite consultar información y realizar trámites con la administración pública.

Acceso seguro

Utiliza sistemas de identificación como certificados digitales o Cl@ve.

Eficiencia centralizada

Ofrece notificaciones y documentos en una plataforma única.

Confidencialidad garantizada

Asegura la protección de datos en todas las interacciones.

Sede Electrónica de la Seguridad Social

Acceso

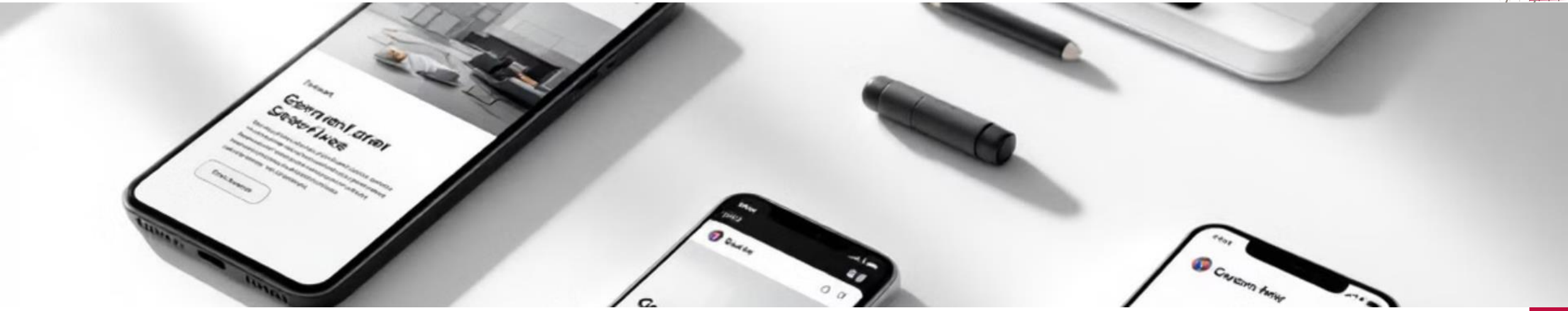
Se requiere certificado digital o Cl@ve para ingresar a la plataforma.

Servicios

Ofrece trámites como solicitud de informes y consulta de datos de cotización.

Ventajas

Disponible 24/7, evita desplazamientos y agiliza los trámites.



Trámites Digitales Comunes

Certificado de empadronamiento

Solicitud en línea a través de la plataforma municipal.

Declaración de la renta

Gestión a través de la web de la Agencia Tributaria.

Vida laboral

Obtención instantánea desde la Sede Electrónica de la Seguridad Social.

Demanda de empleo

Registro y consulta de ofertas en la plataforma del SEPE.

Obtención de la Vida Laboral

- Acceder a la Sede Electrónica de la Seguridad Social.
- Ir a "Ciudadanos" y luego "Informes y Certificados".
- Autenticarse con certificado digital o Cl@ve.
- Solicitar el informe de vida laboral.
- Descargar o imprimir el documento en formato PDF.

Declaración de la Renta Online

Acceso

Entrar en la web de la Agencia Tributaria.

Identificación

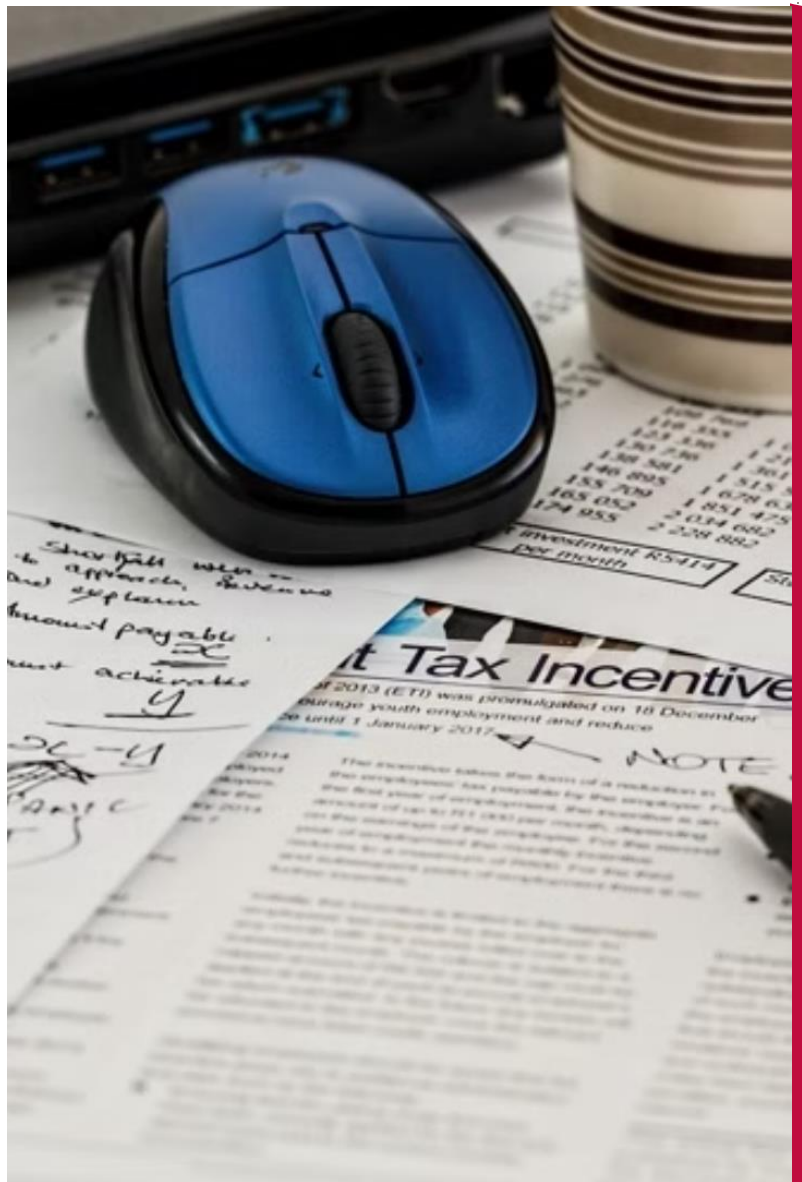
Usar DNI electrónico, Cl@ve o certificado digital.

Revisión

Comprobar el borrador proporcionado por el sistema.

Presentación

Confirmar y enviar la declaración.



Pago de Impuestos Online

Acceso

Entrar en la sección "Pagos" de la Agencia Tributaria.

Selección

Elegir el impuesto o tasa a pagar.

Datos

Introducir información personal e importe.

Pago

Seleccionar método de pago y confirmar.

Certificados Fiscales Digitales

Acceso

Entrar en la web de la Agencia Tributaria e identificarse.

Selección

Buscar la opción "Certificados" y elegir el necesario.

Obtención

Descargar o imprimir el certificado directamente.

Usos

Útil para becas, ayudas o demostrar situación fiscal.

Domiciliación de Impuestos

Acceso

Entrar en "Gestión de deudas" de la Agencia Tributaria.

Selección

Elegir "Domiciliación bancaria".

Datos

Introducir información de la cuenta bancaria.

Confirmación

Verificar y aceptar la domiciliación.

Práctica Guiada: Certificado de Empadronamiento

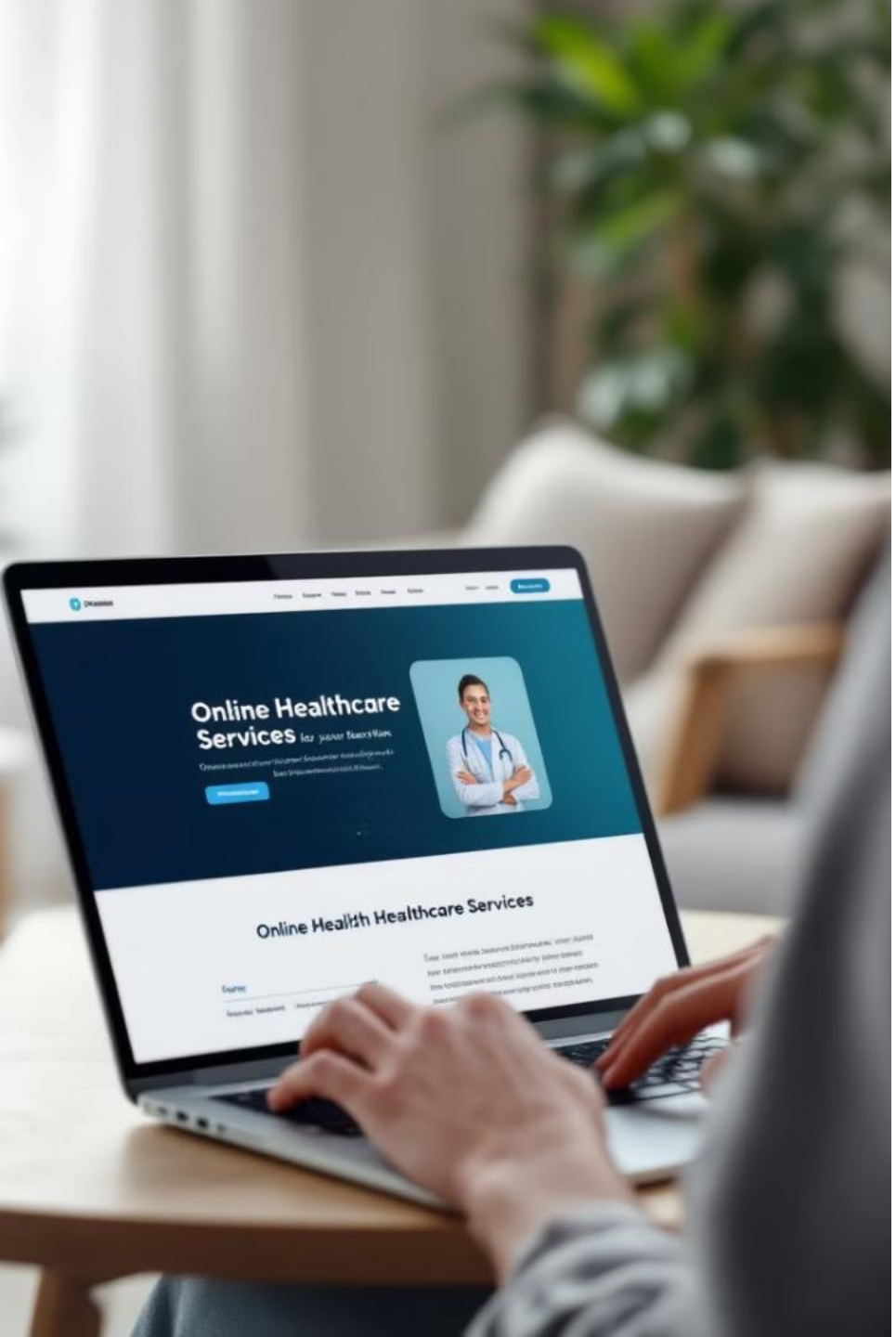
01. Acceder a la Sede Electrónica del Ayuntamiento.

02. Buscar la sección de Trámites o Certificados.

03. Seleccionar "Certificado de Empadronamiento".

04. Identificarse con DNI electrónico o Cl@ve o Certificado Digital.

05. Seguir las indicaciones para descargar el certificado.



Gestión Sanitaria Online: Trámites Fáciles y Seguros

Descubre cómo realizar trámites sanitarios desde casa usando Internet. Aprenderás sobre herramientas como el DNI electrónico y el sistema Cl@ve para acceder de forma segura a tus datos médicos y gestionar citas online.

Ventajas de la Gestión Sanitaria Online

Ahorro de Tiempo

Realiza trámites desde casa sin desplazamientos innecesarios.

Acceso 24/7

Gestiona tus asuntos sanitarios en cualquier momento del día.

Mejor Control

Lleva un seguimiento más preciso de tu información médica.

Identificación Segura

Utiliza herramientas como DNIe y Cl@ve para proteger tus datos.

Servicios Sanitarios Online Disponibles

Cita Previa

Solicita, modifica o cancela citas médicas fácilmente.

Historia Clínica

Accede a tus diagnósticos, tratamientos y antecedentes médicos.

Receta Electrónica

Renueva y consulta tus recetas de medicamentos.

Resultados de Pruebas

Consulta análisis de sangre, radiografías y otros informes médicos.

Pagos Digitales y Gestión Financiera Online

Métodos de Pago Digital

Tarjetas bancarias

Permiten realizar compras online y en tiendas físicas con facilidad.

Transferencias bancarias

Envían dinero directamente entre cuentas bancarias de forma segura.

Aplicaciones móviles

Como Bizum o PayPal, facilitan pagos rápidos desde el teléfono.

Billeteras Electrónicas

PayPal

Plataforma global para pagos seguros y transferencias de dinero online.

Google Pay

Facilita pagos en tiendas físicas y online con dispositivos Android.

Apple Pay

Permite transacciones seguras en dispositivos iOS sin tarjeta física.

Transferencias Bancarias Móviles

Rapidez

Permiten enviar dinero de forma instantánea entre cuentas bancarias.

Comodidad

Realizables desde cualquier lugar a través de apps bancarias.

Seguridad

Utilizan medidas de autenticación avanzadas para proteger las transacciones.

Criptomonedas

Bitcoin

La criptomoneda más conocida, ofrece transacciones descentralizadas y globales.

Ethereum

Plataforma para aplicaciones descentralizadas y contratos inteligentes.

Plataformas de Intercambio

Coinbase y Binance facilitan la compra y venta de criptomonedas.

Transferencias Bancarias y Domiciliaciones

Solicitud de Transferencia

El usuario inicia la transacción desde su banca online o app.

Procesamiento

El banco verifica y ejecuta la transferencia de fondos.

Confirmación

El beneficiario recibe los fondos en su cuenta bancaria.

Seguridad en Pagos Online

Autenticación Multifactor

Añade capas adicionales de seguridad en las transacciones.

Encriptación

Protege la información sensible durante la transmisión de datos.

Monitoreo Continuo

Detecta y previene actividades fraudulentas en tiempo real.

Futuro de los Pagos Digitales

Pagos Biométricos

Transacciones autorizadas mediante huellas dactilares o reconocimiento facial.

Realidad Aumentada

Integración de compras y pagos en experiencias de realidad aumentada.

Blockchain

Mayor adopción de tecnología blockchain para transacciones seguras y transparentes.

Ciberseguridad para Principiantes

Seguridad y Privacidad en la Navegación Web

Borrar el historial, cookies y contraseñas es esencial para proteger tu privacidad y seguridad en línea. Esta práctica mejora la experiencia de navegación y previene accesos no autorizados a tus datos personales.

Importancia de la Limpieza Digital

1

Protección de Datos

Reduce el riesgo de acceso no autorizado a información personal.

2

Mejora del Rendimiento

Ayuda a que las páginas web se carguen más rápido.

3

Prevención de Fraudes

Evita accesos no deseados a tus cuentas en línea.

Paso a Paso: Borrar Historial en Chrome

- **Abrir Chrome**

Haz clic en el icono de Google Chrome en tu escritorio.

- **Menú de Configuración**

Pulsa los tres puntos verticales en la esquina superior derecha.

- **Acceder a Privacidad**

Selecciona "Configuración" y luego "Privacidad y seguridad".

Borrar Datos de Navegación

Seleccionar Datos

Marca las casillas de historial, cookies y caché.

Elegir Intervalo

Selecciona "Todo el tiempo" para borrar todo el historial.

Confirmar

Haz clic en "Borrar datos" para finalizar el proceso.

Eliminar contraseñas guardadas

- **Acceder a Contraseñas**

Ve a "Autocompletar y contraseñas" en la configuración.

- **Localizar Contraseñas**

Busca la lista de contraseñas guardadas.

- **Eliminar**

Haz clic en los tres puntos y selecciona "Eliminar" para cada contraseña.

Introducción a la Ciberseguridad y la Ingeniería Social

Ciberseguridad

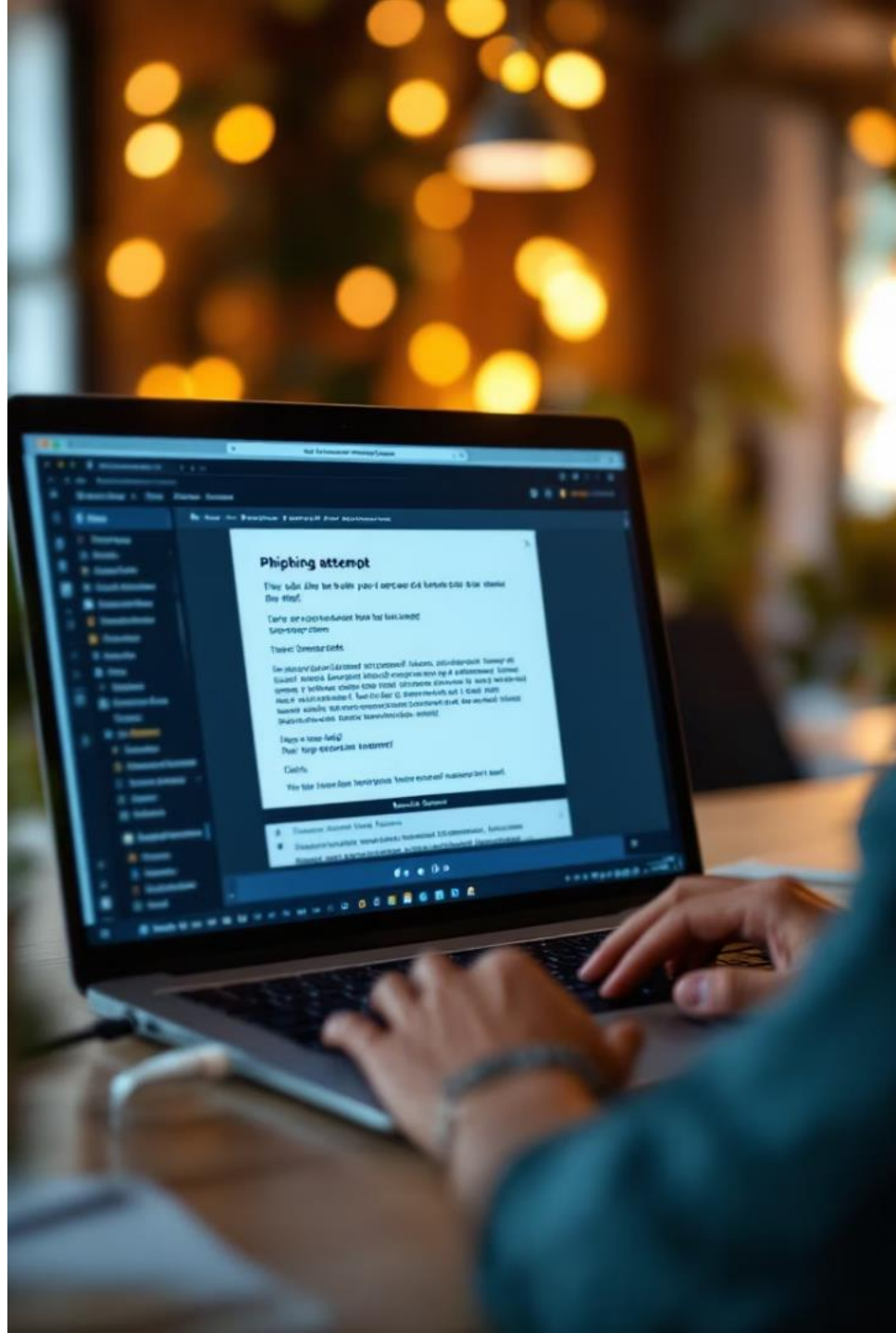
Prácticas para proteger dispositivos, datos y privacidad en internet. Es como cerrar con llave tu casa para evitar riesgos como robo de identidad, estafas y virus. Según **INCIBE** (2024), el 90% de los ciberataques en España involucran engaños humanos.

Ingeniería Social

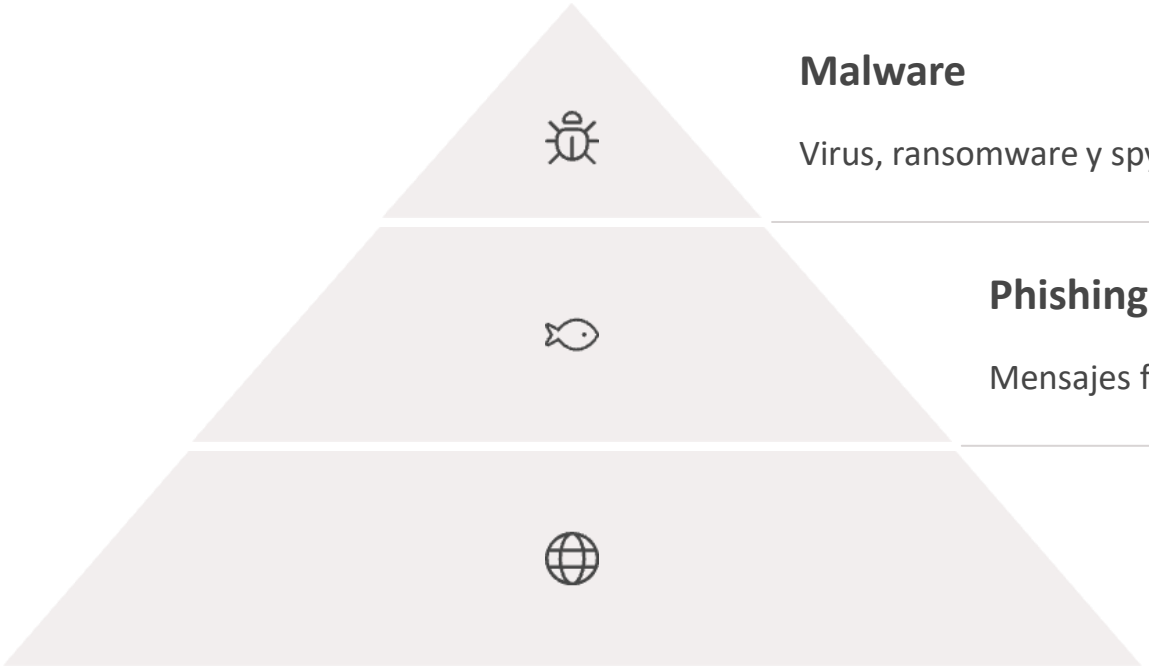
Técnicas para **manipular a personas y personas y obtener información**. Incluye **phishing** (correos falsos), **pretexting** (llamadas de supuestos técnicos) y **baiting** (anuncios engañosos engañosos que piden datos personales). personales).

Señales de Alerta

Aprenderás a identificar remitentes extraños, enlaces sospechosos, tonos urgentes y errores urgentes y errores ortográficos que indican posibles estafas.



Identificar Amenazas en Internet



Malware

Virus, ransomware y spyware que dañan o roban datos

Phishing

Mensajes fraudulentos por correo, SMS o WhatsApp

Sitios Web Falsos

Páginas que imitan bancos o tiendas oficiales

Las amenazas en internet son diversas y cada vez más sofisticadas. El **malware** puede instalarse al descargar un simple "juego gratis". El **phishing** utiliza mensajes como "Tu paquete está retenido, paga 2€ aquí: paquetexpress.xyz". Los **sitios web falsos** imitan páginas legítimas con URLs ligeramente modificadas.

Las **señales de alerta** incluyen URLs extrañas, ventanas emergentes agresivas y mensajes con tono urgente o promesas exageradas.

Reconocer Fuentes Fiables de Información

Criterios de Fiabilidad

- URL con "https://" y candado de seguridad
- Dominios confiables: ".gov", ".edu", medios reconocidos
- Autor con credenciales verificables
- Información contrastada en varias fuentes

Evitar sitios con anuncios excesivos, errores ortográficos o promesas exageradas es fundamental para protegerse de noticias falsas que pueden llevar a estafas o malware.

El candado, cookies y configuración del sitio.

Y cuidado, aun así, ya están haciendo paginas legales, aunque falsas.

falsas.

La diferencia entre un sitio oficial como "sanidad.gob.es" y uno dudoso como "salud-milagro.xyz" puede ser crucial para tu seguridad online.

Herramientas de Protección de Datos y Ciberseguridad

Contraseñas Seguras

Más de 12 caracteres, combinando letras, números y símbolos

Autenticación de Dos Factores

Segundo paso de verificación para acceder a cuentas

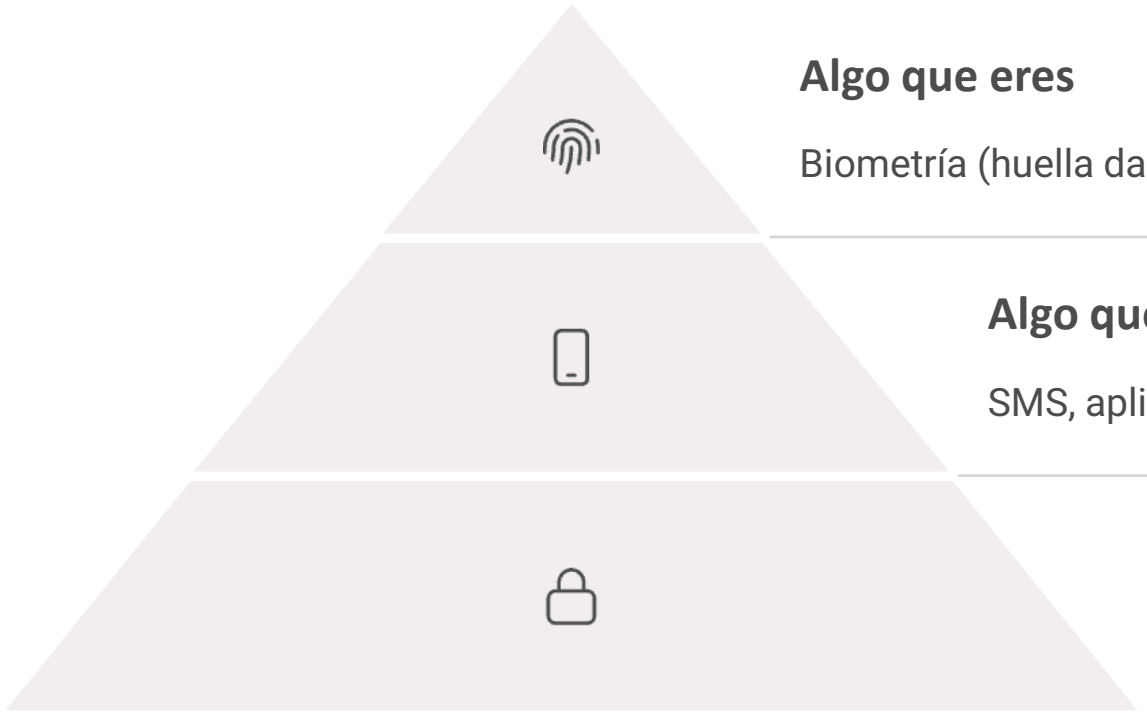
Antivirus y VPN

Protección contra malware y navegación segura

Las **contraseñas seguras** son tu primera línea de defensa. Un ejemplo sería "MeGustaElSol!2025", combinando una frase fácil de recordar con números y símbolos. Los **gestores de contraseñas** como LastPass o Bitwarden pueden ayudarte a mantenerlas organizadas.

La **autenticación de dos factores** añade una capa extra de seguridad, solicitando un código adicional enviado a tu móvil. Es especialmente importante activarla en correo, importante activarla en correo, redes sociales y bancos. Complementa estas medidas con un buen antivirus y una VPN para redes públicas.

Autenticación Multifactor (MFA)



Algo que eres

Biometría (huella dactilar, reconocimiento facial)

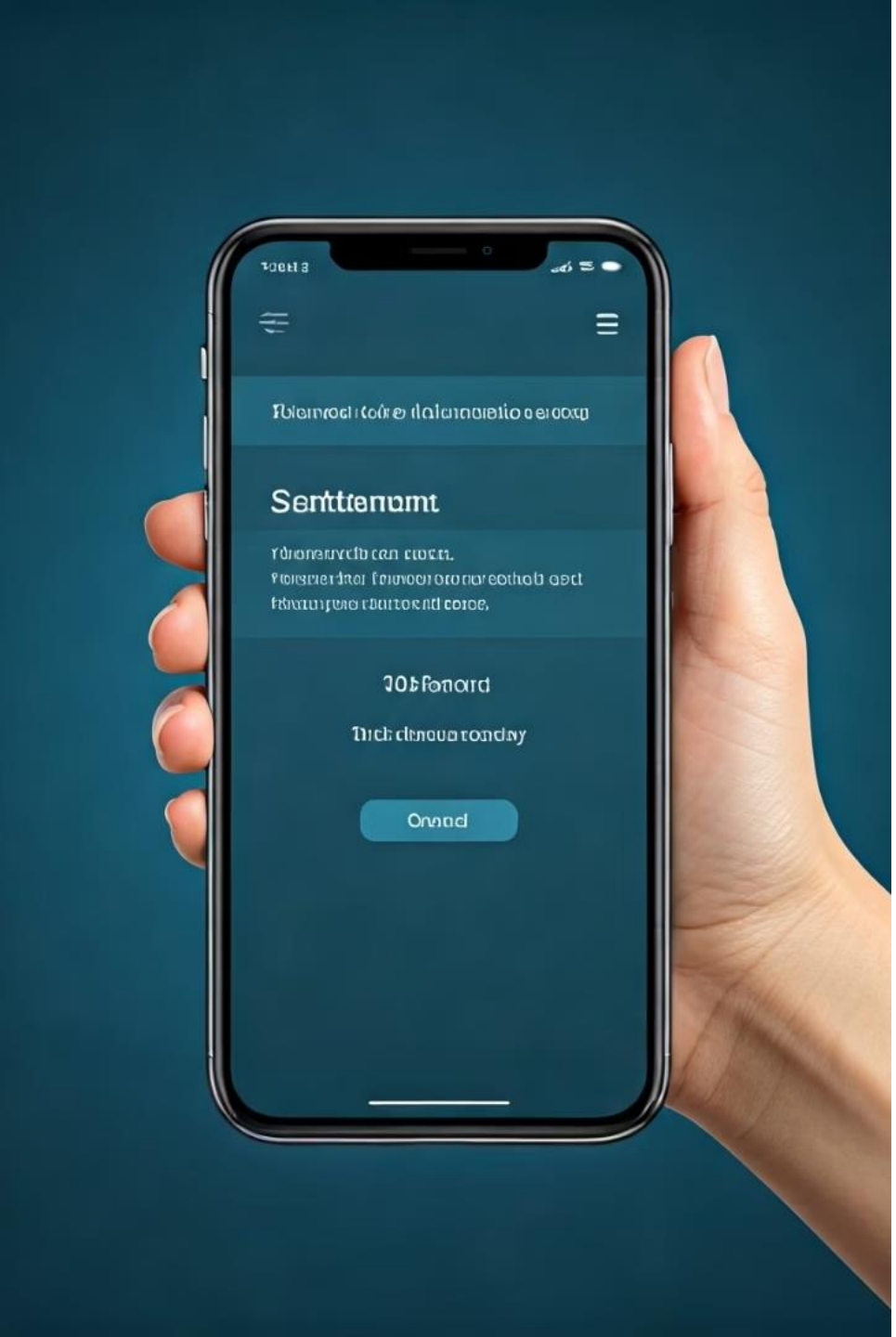
Algo que tienes

SMS, aplicaciones authenticator, tokens físicos

Algo que sabes

Contraseña o PIN

La implementación de MFA reduce el riesgo de accesos no autorizados en un 99.9% según Welivesecurity.
Junto con esto, actualizar el software, nos permite una seguridad casi completa..



Configuración de Autenticación en Dos Pasos

Acceder a Configuración

Dirígete a la sección de seguridad de tu cuenta (Gmail, Facebook, etc.).

Activar 2FA

Selecciona la opción de verificación en dos pasos y elige método (SMS o app).

Guardar Códigos

Almacena los códigos de recuperación en un lugar seguro y accesible.

Errores Comunes y Verificación

Errores Frecuentes

- Reutilizar contraseñas en múltiples servicios
- Usar datos personales identificables
- No actualizar contraseñas periódicamente

Herramientas de Verificación

- Have I Been Pwned
- Servicio Antibotnet
- Verificadores integrados en navegadores

Dato Alarmante

El 80% de los ataques en España durante 2024 se debieron a contraseñas débiles (INCIBE).

Medidas para Evitar Ataques de Ingeniería Social

No hagas clic en enlaces sospechosos

Evita abrir archivos o enlaces de remitentes desconocidos

2

No compartas datos sensibles

Nunca proporciones contraseñas o DNI por correo, SMS o teléfono

Verifica identidades

Llama al número oficial de la empresa para confirmar contactos

Desconfía de urgencias

Los mensajes que exigen acción inmediata suelen ser fraudulentos

La ingeniería social se basa en **manipular a las personas** para obtener información confidencial. Un ejemplo Un ejemplo común es recibir una llamada de alguien que dice ser de "Microsoft" pidiendo acceso remoto a tu remoto a tu ordenador. La respuesta correcta es colgar y verificar por canales oficiales.

Navegación Segura por la Calle y Cuidados a Tener Presentes

Riesgos en Espacios Públicos

- Redes Wi-Fi falsas que espían tus datos
- Robo de dispositivos sin bloqueo
- Espionaje visual de tus contraseñas

Medidas de Protección

- Usar VPN en redes públicas
- Evitar acceder a cuentas sensibles
- Bloquear dispositivos con PIN o biometría

Precauciones Adicionales

- Utilizar protectores de pantalla
- Desactivar Bluetooth y Wi-Fi cuando no se usen
- Realizar copias de seguridad regularmente

Los espacios públicos presentan riesgos únicos para nuestra seguridad digital. Un hacker podría crear una red llamada **"CaféWiFiGratis"**para **"CaféWiFiGratis"**para interceptar tus datos, o alguien podría observar tu **PIN, en el autobús, o en un bar**, mientras lo introduces en un banco. en un banco. Implementar estas medidas te ayudará a proteger tu información personal cuando estés fuera de casa.

Protección Wi-Fi de Casa

Cambiar SSID y Contraseña

Usar nombres no identificables y contraseñas robustas

Activar Cifrado Seguro

Configurar WPA3 o WPA2 y evitar WEP

Proteger el Router

Cambiar contraseña de administrador

Ocultar Red

Desactivar transmisión de SSID

Tu red Wi-Fi doméstica puede ser una puerta de entrada para ciberdelincuentes si no está correctamente configurada. Es recomendable usar **nombres de red genéricos nombres de red genéricos** como "RedSegura25" en lugar de "CasaPérez" que revela tu identidad. La contraseña debe ser robusta, por ejemplo "WiFiSeguro!2025". "WiFiSeguro!2025".

Acceder a la configuración del router (normalmente en 192.168.1.1) te permitirá implementar estas medidas de seguridad.

Protege tus dispositivos IoT contra ciberataques

Los dispositivos conectados como cámaras, altavoces inteligentes y termostatos pueden ser vulnerables. Sin protección adecuada, los hackers podrían espiar tu hogar.

Cambia contraseñas predeterminadas

Sustituye "admin" por combinaciones seguras y únicas.

Actualiza el firmware

Mantén el software de tus dispositivos siempre al día.

Usa una red separada

Conecta tus dispositivos IoT a una red Wi-Fi independiente.

Relojes inteligentes, Impresoras, Aspiradoras Robóticas, Termostatos, Sistemas de Riego, Neveras, Calefacción, cámaras, etc.

Desactiva funciones innecesarias: Ej. Si no usas el micrófono de una cámara, apágalo.

¡Recuerda! Una cámara hackeada podría grabar el interior de tu casa sin que lo sepas.

Adecco
Learning & Consulting

LAS ROZAS
SMART CITY

¡Sois unas cracks digitales!

Espero hayáis pasado un buen rato.

Para mí fue magnifico compartir estas 3 horas con vosotros.

Hasta la próxima

GESTIONES DIGITALES CON LA ADMINISTRACIÓN

13 de ENERO de 2026, 10 am – 13 am

“Proyecto Comunidad Digital ATC-Las Rozas”

AMERICAN TOWER
ESPAÑA

Las Rozas

comunidades digitales