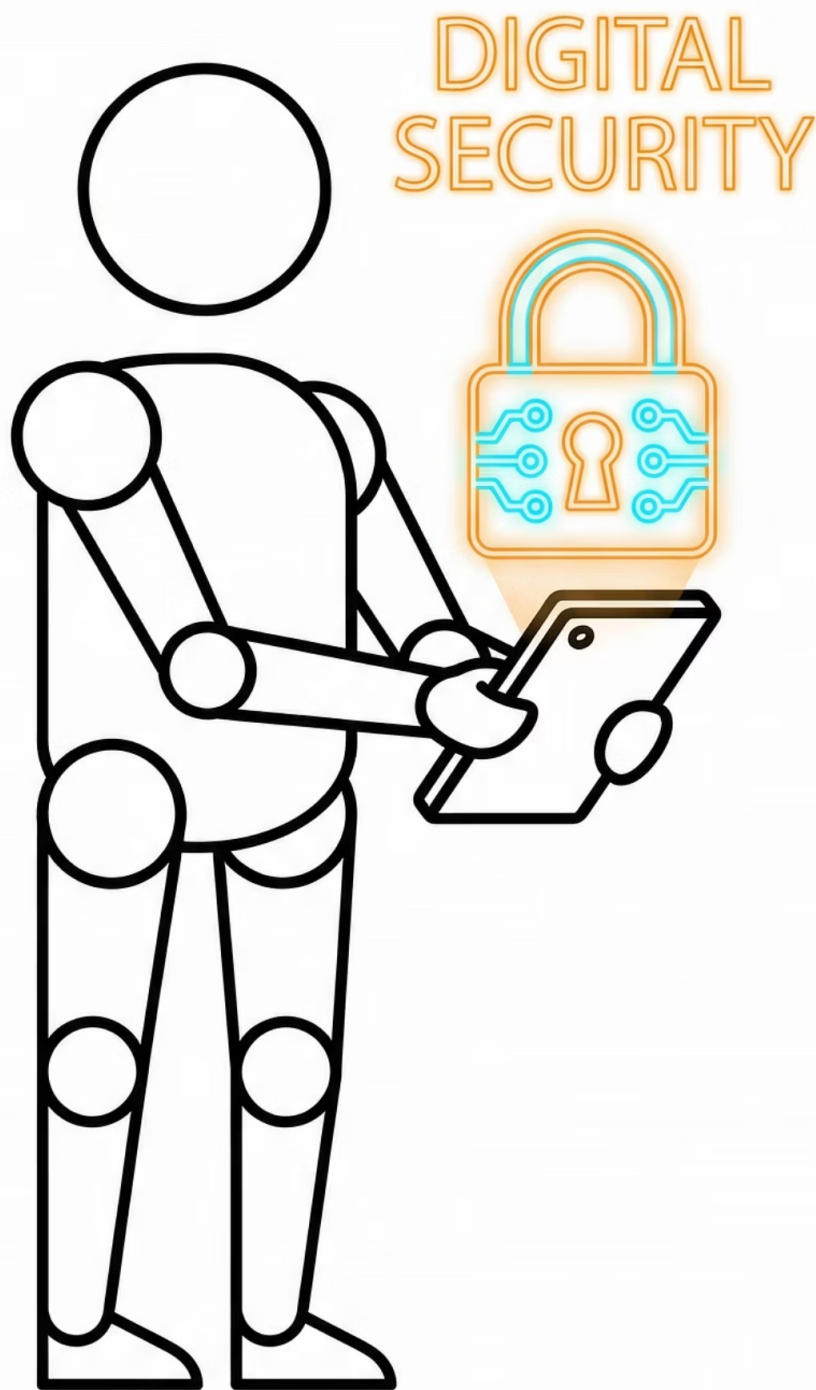




INTRO

As administracións e os provedores de servizos dixitais dan por suposto que todos temos un **dispositivo smartphone**.

No mundo dixital non nos identificamos cun DNI ou pasaporte; os **números de teléfono móbil** e os enderezos de **correo electrónico** serven para identificarnos ou localizarnos.

Para o uso eficaz e seguro dos servizos dixitais os **certificados dixitais** son esenciais; sen eles, é imposible ou moi difícil realizar certos trámites ou acceder a certos servizos.

Os correos electrónicos son unha forma de proba "prima facie", mentres que os correos electrónicos asinados electronicamente teñen plena **validez legal** comparable á dun burofax.

Perfis de Usuario



NON teño teléfono móbil e NON teño ordenador: envexa sana, non vou tentar cambiar a cousa, podería empeoralala.



Teño teléfono móbil e NON teño ordenador: non podo cubrir certos riscos de xeito eficiente, pero poderei acceder á meirande parte dos servizos, aínda que é difícil xestionar e intercambiar documentos.



NON teño teléfono móbil e SÍ teño ordenador: un teléfono móbil melloraría a seguridade con ferramentas de 2FA e a accesibilidade aos servizos.



Teño teléfono móbil e ordenador: isto permíte ter alternativas no caso de que un dos servizos falle, e modos de recuperación ante desastres (copia de seguridade, recuperación de contas, ...).

RECOMENDACIÓN: Teléfono móbil con identificación biométrica (huella dactilar) e NFC.

Primeiros Pasos; Seguridad e Eficiencia



1. Configurar E-mail Principal

Configura unha conta de **correo electrónico**, preferiblemente no teléfono móvil como conta principal. Esta contrasinal inicial non precisa ser forte.



3. Protexer ben o E-mail Principal

Empregando o xestor de contrasinais, xera un contrasinal forte e gárdao como o **contrasinal do correo electrónico**. Despois cambia o **contrasinal inicial** (punto 1) no Gmail.



2. Gestor de contrasinais

A **contrasinal mestra** de acceso debe ser forte. Para máis comodidade, podemos habilitar o acceso coa identificación de pegadas dactilares biométricas.



4. Certificado Dixital

Solicita un **certificado dixital** de persoa física á FNMT. Emprega o enderezo de correo electrónico anterior.

Descargado o certificado, gárdao cun contrasinal forte xerado co xestor de contrasinais. Iste queda gardado no propio xestor de contrasinais.

Cimentos robustos

Necesitaremos contrasinais para acceder a servizos dixitais e tamén para cifrar datos sensibles, como a parte privada do noso certificado dixital ou o ficheiro que contén decenas de contrasinais para cada servizo.



Contrasinais Robusta

Mínimo de 16 caracteres. Misture maiúsculas, minúsculas, números e símbolos. Nunca use datos persoais.



Keepass, un xestor de contrasinais con todos os requisitos mínimos

1. cifrado de grao militar (AES-256, ChaCha20).
2. código aberto.
3. almacenamento local do ficheiro onde se gardan todos os contrasinais.



Unha Contrasinal por Servizo/Conta

Nunca repita contrasinais. Se un servizo se ve comprometido, os outros permanecen seguros.



A contrasinal do xestor de contrasinais é un dos pilares da seguridade

É irrenunciable que cumpra cos criterios de contrasinal robusta, xa que é a chave para acceder ás demais contrasinais.



A contrasinal Maestra do Xestor de Contrasinais

A contrasinal mestra para acceder ao xestor de contrasinais debe tratarse con sumo coidado, seguindo escrupulosamente as recomendacións feitas anteriormente para contrasinais robustas e resistindo á tentación de anotala nun ficheiro ou nunha nota adhesiva.

Se tes medo de perder a memoria, emprega a túa imaxinación (steganografía), tendo en conta que as opcións non dixitais (por exemplo escribir en papel) supoñen problemas adicionais se a contrasinal contén letras maiúsculas, ceros, guións, etc.

Exemplo de contrasinal mestra: “_@#gbgaaa#@-_16”.



Certificado Dixital FNMT

Os certificados de "persoa física" / usuario emitidos pola FNMT-RCM permiten comunicarse coas diversas administracións empregando un único certificado.

O certificado instálase no seu teléfono, ordenador ou dispositivo sen necesidade de ningún periférico (lector físico, token ...).

O proceso de obtención do certificado na FNMT (como un ficheiro descargable) divídese en catro pasos:

1. Configuración

Para solicitar o certificado, necesitas instalar software seguindo indicacións da FNMT (Autofirm@).

2. Solicitud en liña

Unha vez que complete a solicitud, recibirá un Código de solicitud na súa conta de correo electrónico, que será necesario cando verifique a súa identidade e máis tarde cando descargue o seu certificado.

3. Acreditación presencial

Oficina de Acreditación de Identidade: INSS de Ribadeo (C/ Irmáns Moreno Ulloa, 4) ou no Concello

4. Descarga do Certificado

Descarga desde a web da FNMT, e copia de seguridade do certificado cunha clave de acceso segura.

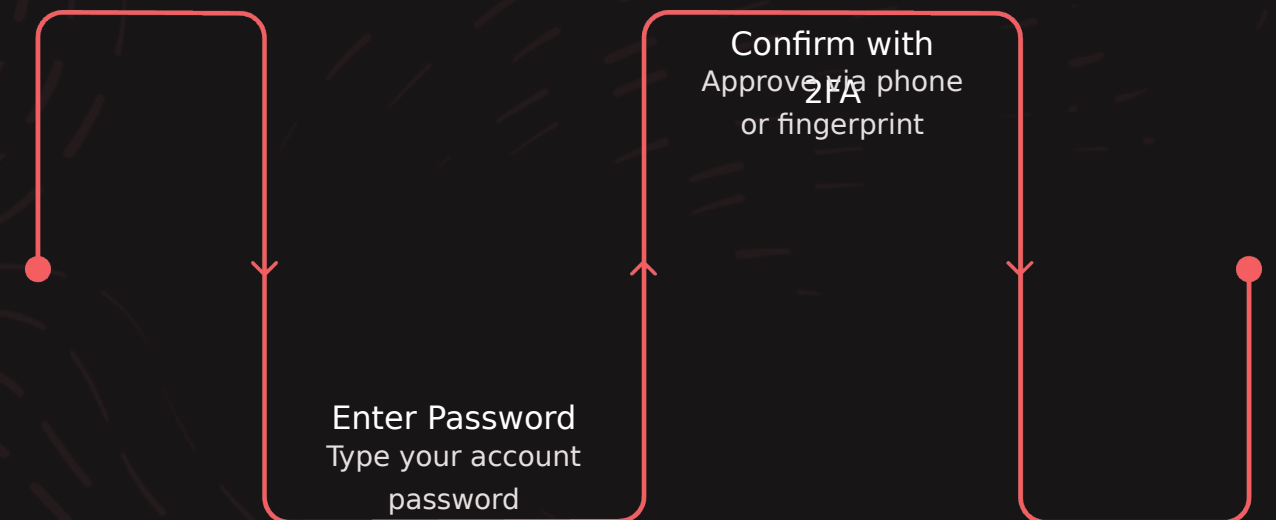
Banca Electrónica, Dir. UE PSD2 e Autenticación

Directiva de Servicios de Pago

A Directiva UE PSD2 obliga as entidades a implementar a autenticación de doble factor (2FA).

Autenticación de doble factor (2FA). Factores:

1. algo que se coñece (combinación de nome de usuario/contrasinal)
2. algo que posúes, algo físico dispoñible só para o usuario (móbil, token, DNI ou pasaporte)
3. algo que es, como datos biométricos (huella dactilar, iris ou cara)



Boas Prácticas, Recomendacións

Número Vitalício

Conserve o mesmo número de teléfono móbil para sempre; é parte da nosa identidade dixital.

E-mail principal

Configure notificacións por correo electrónico para asuntos oficiais, de organismos públicos, banca on-line ou para certificados dixitais (renovación).

Pagamentos

Levar tarxetas de crédito no móbil con aplicacións como *Wallet* é máis seguro que pagar con tarxetas físicas.

Facer compras en liña con tarxetas virtuais e/ou de un só uso aumenta a seguridade dos nosos pagos.

E-mails secundario/s

Para asuntos como compras, redes sociais, etc., ten unha segunda conta de correo electrónico; isto axudarache a evitar o spam e outros riscos que poderían comprometer a túa seguridade.

Biometría Activa

Ative sempre a autenticación con biometría, p.e. pegada dixital, e a autenticación de dous factores (2FA) en cada un dos servizos se estes o permiten.

Documentos oficiais versión dixital

Garda no teu dispositivo versións dixitais do teu DNI (MiDNI) e da túa tarxeta sanitaria (Sergas Móbil).

Servizos Dixitais



Cl@ve / Ch@ve 365

miDNI



miDGT

Carnet de conducir, puntos, multas



Certificado digital
FNMT



Sergas Móbil

Tarxeta sanitaria, citas, historial, TELEA (asistencia domiciliaria), reclamacións e acheas



Gestión

Mi carpeta ciudadana e **Notifica app** para centralizar avisos e documentos oficiais.

DEHU



Importass

Certificados, pagos a SS, vida laboral, cotizaciones

Recuerda



Configura unha conta de **correo electrónico**, preferiblemente no teu teléfono móbil Android.

PRIMEIROS PASOS



Instala un **xestor de contrasinais**. A contrasinal mestra de acceso debe ser forte.



Xera un **contrasinal forte** como contrasinal de Gmail para a conta de Android, e cambia o contrasinal inicial.



Solicita un certificado dixital de persoa física á FNMT. Gárdao cun contrasinal forte xerado e gardado no xestor de contrasinais.

Grazas pola asistencia

Descarga de blogs.amarinha.gal todos os fanzines

