INCLUSIVE DIGITAL BANKING:
EMPOWERING SENIORS WITH DIGITAL SKILLS

2024-1-ES01-KA210-ADU-000243084

INFORMACIÓN DE SEGURIDAD DIGITAL EN ESPAÑA

TABLA DE REVISIÓN DE CALIDAD

Reseña	Fecha	Descripción de la modificación	Firma
0	31/10/2025	Redacción original	

AVISO LEGAL

Cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados son únicamente de los autores y no reflejan necesariamente los de la Unión Europea ni del Servicio Español para la Internacionalización de la Educación (SEPIE). Ni la Unión Europea ni la autoridad que otorga la autoridad pueden ser responsables de ellos.

Cofinanciado por la Unión Europea

LICENCIA CREATIVE COMMONS

ÍNDICE

INFORMACIÓN DE SEGURIDAD DIGITAL EN ESPAÑA 3

1. INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE) 3

2. LEYES DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD EN ESPAÑA 3

3. CONCIENCIACIÓN SOBRE CIBERSEGURIDAD ENTRE LOS RESPONSABLES DE LA TOMA DE DECISIONES 4

4. ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 4

5. INCIBE-CERT: EQUIPO ESPAÑOL DE RESPUESTA A EMERGENCIAS INFORMÁTICAS 5

6. CL@VE Y CONCIENCIACIÓN DE LA AGENCIA TRIBUTARIA 5

7. CERTIFICADOS DIGITALES (POR EJEMPLO, FNMT-RCM) 5

8. CL@VE 5

9. APLICACIONES DE AUTENTICACIÓN DE BANCOS MÓVILES 6

10. CAMPAÑAS Y HERRAMIENTAS DE REPORTE DE CERTIFICACIÓN EN ESPAÑA 6

11. TENDENCIAS RECIENTES EN ESPAÑA (2023–2025) 6

BIBLIOGRAFÍA 7

INFORMACIÓN DE SEGURIDAD DIGITAL EN ESPAÑA

En España, la orientación en seguridad digital es proporcionada activamente por INCIBE (Instituto Nacional de Ciberseguridad), que ofrece recursos dedicados y una línea de ayuda (017) para personas que enfrentan dificultades en línea (INCIBE, s.f.). También ha creado un canal prioritario de asistencia telefónica para adultos mayores, ayudándoles a abordar los problemas de ciberseguridad con un apoyo personalizado (Tendencias, 2023).

Se recomienda a los usuarios mayores evitar hacer clic en enlaces sospechosos, especialmente en mensajes que pidan datos personales o bancarios, y acceder a sitios web oficiales. Los bancos españoles también dependen de sistemas seguros de verificación en dos pasos (2FA), a menudo mediante códigos SMS o identificación biométrica.

1. INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE)

INCIBE (Instituto Nacional de Ciberseguridad) es la autoridad central en ciberseguridad en España, bajo el Ministerio de Transformación Digital y Administración Pública. Coordina las estrategias nacionales de ciberseguridad, ofrece apoyo a ciudadanos, empresas y operadores esenciales, y actúa como punto de contacto con redes europeas como ENISA (Agencia Europea de Ciberseguridad).

INCIBE trabaja estrechamente con organizaciones como CCN-CERT (para sistemas del sector público) y gestiona iniciativas clave como CERTSI, que supervisa amenazas y coordina la respuesta a incidentes en toda España. Es una herramienta gubernamental destinada a desarrollar la ciberseguridad como motor de transformación social e innovación, centrada en la investigación, la prestación de servicios y la coordinación con los actores relevantes. También es una entidad clave para promover la confianza digital entre ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente en sectores estratégicos (INCIBE, s.f.).

2. LEYES DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD EN ESPAÑA

El marco legal de España para la protección de datos y la ciberseguridad incluye:

- **Ley Orgánica 3/2018 sobre Protección de Datos y Garantía de Derechos Digitales (LOPDGDD):** Se alinea con el Reglamento General de Protección de Datos (RGPD) de la UE, que establece principios de protección de datos y derechos individuales.

- **Marco Nacional de Ciberseguridad (Ley 12/2018):** Implementa la Directiva NIS de la UE, centrada en la seguridad de los sistemas de red e información.
- **Real Decreto 704/2017 sobre el Esquema Nacional de Seguridad (ENS):** Proporciona la base para la seguridad de la información dentro de organizaciones del sector público y operadores de infraestructuras críticas (Comisión Europea, 2019; García, 2021).

3. CONCIENCIACIÓN SOBRE CIBERSEGURIDAD ENTRE LOS RESPONSABLES DE LA TOMA DE DECISIONES

Un estudio realizado por Del Real (2025) muestra una preocupante brecha en la conciencia sobre ciberseguridad identificada entre los responsables de la toma de decisiones en España, especialmente aquellos sin formación técnica. A través del método Delphi, los expertos consultados coincidieron en que esta falta de conocimiento supone una barrera significativa para la gobernanza eficaz del ecosistema digital.

Los líderes políticos y empresariales de alto nivel a menudo no comprenden plenamente la naturaleza multidimensional de las amenazas cibernéticas ni sus implicaciones legales y estratégicas. Como respuesta, el estudio subraya la urgente necesidad de implementar programas de formación específicos y centralizar los esfuerzos de concienciación institucional dentro de una futura autoridad nacional de ciberseguridad. Una entidad así ayudaría a cerrar la brecha entre las capacidades técnicas y la toma de decisiones políticas, fomentando una cultura organizacional más informada y resiliente para afrontar los nuevos desafíos digitales (Del-Real, C. y Díaz-Fernández, A.M., 2025).

4. ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

España cuenta con una Estrategia Nacional de Ciberseguridad que se publicó por primera vez en 2013 y se actualizó en 2019. La estrategia pretende garantizar que España haga un uso seguro de los sistemas de información y telecomunicaciones y reforcer las acciones de prevención, defensa, detección, respuesta y recuperación de ciberataques frente a las amenazas cibernéticas.

La estrategia se centra en cinco objetivos principales: mejorar las habilidades para contrarrestar las amenazas cibernéticas, garantizar la seguridad de activos estratégicos, mejorar la ciberseguridad para ciudadanos y empresas, fortalecer las capacidades para investigar y procesar los ciberdelitos y contribuir a los esfuerzos internacionales de ciberseguridad. También promueve una cultura de ciberseguridad que enfatiza la concienciación, la educación y las mejores prácticas en todos los sectores (Dig.watch, 2019).

5. INCIBE-CERT: EQUIPO ESPAÑOL DE RESPUESTA A EMERGENCIAS INFORMÁTICAS

INCIBE-CERT es el centro de referencia de respuesta a incidentes de seguridad para ciudadanos y entidades de derecho privado en España, gestionado por el Instituto Nacional de Ciberseguridad de España (INCIBE), bajo el Ministerio de Economía y Transformación Digital, a través de la Secretaría de Estado de Digitalización y Servicio Público (INCIBE-CERT, s.f.).

6. CL@VE Y CONCIENCIACIÓN DE LA AGENCIA TRIBUTARIA

En España, muchos usuarios dependen de Cl@ve y las plataformas de la Agencia Tributaria para servicios de identidad digital y fiscales. Es fundamental recordar a los usuarios que los ataques de phishing imitan frecuentemente estos servicios oficiales, por lo que nunca deben introducir sus credenciales a través de enlaces recibidos por correo electrónico o SMS (INCIBE, s.f.).

7. CERTIFICADOS DIGITALES (POR EJEMPLO, FNMT-RCM)

España utiliza certificados digitales emitidos por entidades como la FNMT-RCM (Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda) para identificación digital segura y firmas electrónicas. Es esencial almacenar estos certificados de forma segura, mantener copias de seguridad y asegurarse de que se renuevan antes de la expiración (FNMT-RCM, s.f.).

8. CL@VE

Cl@ve es el sistema oficial de identificación y autenticación en línea de España, diseñado para proporcionar acceso seguro a una amplia gama de servicios digitales públicos utilizando un único conjunto de credenciales. Permite a los usuarios iniciar sesión de forma segura en plataformas gubernamentales, firmar documentos electrónicamente y acceder a información personal y procedimientos administrativos.

¿Por qué se usa Cl@ve?

- Para acceder de forma segura a servicios como la Agencia Tributaria, la DGT y la Seguridad Social.
- Firmar documentos y solicitudes digitalmente a través de Cl@ve Firma.
- Para simplificar la autenticación en múltiples sitios web de la administración pública.

- Utilizar métodos de autenticación de dos pasos, como códigos SMS o la aplicación PIN Cl@ve.

Cl@ve soporta varios métodos de inicio de sesión, entre ellos:

- DNIe (DNIe (identificación nacional electrónica).
- Cl@ve PIN (inicio de sesión temporal basado en SMS).
- Cl@ve Permanente (contraseña + segundo factor).
- Certificados digitales (por ejemplo, FNMT-RCM).
- Identificación biométrica (a través de dispositivos móviles compatibles) (Cl@ve, s.f.).

9. APLICACIONES DE AUTENTICACIÓN DE BANCOS MÓVILES

Los bancos españoles (por ejemplo, BBVA, Santander, CaixaBank) utilizan aplicaciones (por ejemplo, BBVA Wallet, Santander Wallet, CaixaBankNow) para acceder de forma segura y aprobar transacciones. Estas aplicaciones deben descargarse desde las tiendas oficiales y tener la biometría o PIN activados para mayor seguridad.

10. CAMPAÑAS Y HERRAMIENTAS DE REPORTE DE CERTIFICACIÓN EN ESPAÑA

CERT España gestiona el portal nacional https://www.incibe.es/ciudadania/ayuda/reporte-de-fraude, donde los usuarios pueden denunciar contenido sospechoso. El sitio ofrece concienciación sobre ciberseguridad, alertas de estafas y ejemplos de phishing (INCIBE, s.f.).

11. TENDENCIAS RECIENTES EN ESPAÑA (2023–2025)

- **Aumento de vishing y smishing:** Los atacantes se hacen pasar por empleados bancarios mediante llamadas telefónicas o SMS para robar información personal, con incidentes notables en Zaragoza (2025) (cadenaser.com).
- **Estafas de deep fake de voz:** Los delincuentes usaron voces generadas por IA para hacerse pasar por el asistente virtual de Vodafone en las Islas Canarias (2024) (huffingtonpost.es).
- **Fraude en compras online:** Un grupo defraudó a más de 1.000 víctimas creando sitios de comercio electrónico falsos que vendían electrónica (2024) (elpais.com).

BIBLIOGRAFÍA

Comisión Europea (2019). *Hoja informativa sobre Gobierno Digital 2019*:

→ Chrome-extension://efaidnbmnnnibpcajpcpcglclefindmkaj/https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Slovenia_2019_0.pdf

Banco de España (2020). *Seguridad y recomendaciones de la banca móvil*:

→ https://www.bde.es

Cadenaser (2025). *Seis detenidos en Zaragoza por estafar más de 100.000 euros a 53 personas*:

→ https://cadenaser.com

Del-Real, C., & Díaz-Fernández, A. M. (2025). *¿Quién gobernará la ciberseguridad en España para 2035? Resultados de un estudio de Delphi.* Ciencia de futuros y previsión, 7, e208:

→ https://doi.org/10.1002/ffo2.208

Dig.watch (abril de 2019). *La Estrategia Nacional de Ciberseguridad de España*:

→ https://dig.watch/resource/spains-national-cybersecurity-strategy

El País (2024). *Una red criminal estafó cinco millones a más de 1,000 víctimas en ventas en línea de tecnología de alta gama*:

→ https://elpais.com

Comisión Europea (2019). *Hoja informativa sobre Gobierno Digital 2019 España*:

→ https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Spain_2019_1.pdf

FNMT-RCM. (s.f.). *Certificados digitales. Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda*:

→ https://www.sede.fnmt.gob.es/certificados

García, J. (2021). *La Estrategia de Seguridad Nacional 2021 y la National Security Strategy 2022: una visión compartida.* Dialnet:

→ https://dialnet.unirioja.es/servlet/articulo?codigo=9049920

Gobierno de España (s.f.). *Sistema Cl@ve*.

→ https://clave.gob.es

Huffingtonpost (2024). *La estafa Vodafone comenzada en Canarias*.

→ https://www.huffingtonpost.es

INCIBE (s.f.-a). *Consejos de ciberseguridad para ciudadanos. Instituto Nacional de Ciberseguridad*.

→ https://www.incibe.es

INCIBE (s.f.-b). *Herramientas de ciberseguridad y reportes. Instituto Nacional de Ciberseguridad*.

→ https://www.incibe.es

Trendencias (2023). *Cómo actuar ante las ciberestafas: el teléfono 017 de INCIBE abre un canal prioritario para personas mayores*.

→ https://www.trendencias.com/silver/como-actuar-ciberestafas-telefono-017-incibe-abre-canal-prioritario-para-personas-mayores

Este documento ha sido desarrollado por este...

CONSORCIO

LÍDER

HORIZONTE XXII (España)

SOCIOS

LJUDSKA UNIVERZA, ZAVOD ZA IZOBRAZEVANJE IN KULTURO, ROGASKA SLATINA (Eslovenia)

EGESTIONPYME INTERNET S.L. (España)

KULTUR EGITIM VE PROJE DERNEGI - KEPDER (Turquía)