ESPAÑA EFICIENTE

POLICY BRIEF | SEGURIDAD NACIONAL DIGITAL

Ciberseguridad Nacional: Protección de Infraestructuras, Ciudadanos y Soberanía Digital

Un ataque cibernético a una central eléctrica, un hospital o el sistema financiero no necesita ejercito ni armas.

Necesita un ordenador y una vulnerabilidad sin parchear.

La ciberseguridad es la defensa nacional del siglo XXI.

1. Resumen Ejecutivo

España es uno de los países europeos con mayor numero de ciberataques registrados anualmente. Sus infraestructuras criticas, administraciones publicas, empresas estratégicas y ciudadanos son objetivos permanentes de actores estatales hostiles, grupos criminales organizados y hacktivistas. Al mismo tiempo, España Eficiente ha desarrollado un conjunto de sistemas digitales que son pilares del modelo: la app GIF, el sistema ROC, la app AUXILIA, el DVO, la tarjeta sanitaria única, las oficinas hibridas de protección ciudadana y el dashboard de transparencia del gasto publico. Todos estos sistemas dependen de infraestructura digital que debe estar protegida. La ciberseguridad no es una política accesoria de España Eficiente. Es una condición necesaria para que todo lo demás funcione. Este documento propone un modelo de ciberseguridad nacional en cuatro pilares: protección de infraestructuras criticas, defensa del ciudadano digital, soberanía tecnológica y talento nacional en ciberseguridad.

2. La Amenaza: Concreta, Creciente y Subestimada

- España figura entre los diez países europeos con mayor volumen de ciberataques anuales según los informes del Centro Nacional de Inteligencia (CNI) y del INCIBE.
- Los ataques de ransomware a hospitales, ayuntamientos y empresas publicas españolas han paralizado servicios críticos durante días en casos documentados recientes.
- Los actores estatales hostiles (principalmente Rusia, China y grupos vinculados a Irán y Corea del Norte) realizan operaciones permanentes de espionaje, desinformación y sabotaje digital contra objetivos españoles.
- El coste económico del cibercriminal en España se estima en varios miles de millones de euros anuales incluyendo fraudes, ransomware, robo de datos y sabotaje industrial.
- La superficie de ataque crece cada ano: mas dispositivos conectados, mas servicios digitales públicos, mas datos sensibles en sistemas informáticos. Cada nuevo servicio digital es una nueva puerta de entrada potencial.

Todos los sistemas digitales de España Eficiente (GIF, AUXILIA, DVO, tarjeta sanitaria, dashboard de gasto) son objetivos potenciales de ciberataques.
Sin ciberseguridad robusta, la digitalización del Estado es una vulnerabilidad, no una fortaleza.

3. Las Infraestructuras Criticas: Prioridad Absoluta

Las infraestructuras criticas son aquellas cuya interrupción tendría consecuencias graves para la seguridad nacional, la economía o el bienestar de la población:

Infraestructura critica	Riesgo cibernético	Medida de protección prioritaria
Red eléctrica nacional	Ataque puede dejar sin suministro a millones de personas durante días.	Segmentación de redes. Sistemas de control industrial aislados de internet. Redundancia.
Sistema financiero y bancario	Ataque puede bloquear pagos, transferencias y acceso a cuentas.	Auditorias de seguridad obligatorias. Protocolo de respuesta en menos de 2 horas.
Hospitales y sistema sanitario	Ransomware puede paralizar quirófanos y registros médicos poniendo vidas en riesgo.	Copias de seguridad aisladas. Protocolo de continuidad offline. Cifrado de historiales.
Sistema GIF y administración fiscal	Ataque puede comprometer datos fiscales de millones de empresas y ciudadanos.	Arquitectura de seguridad por capas. Autenticación multifactorial obligatoria.
Redes de agua y saneamiento	Manipulación de sistemas SCADA puede contaminar suministros.	Redes de control completamente aisladas. Monitorización 24/7.
Comunicaciones y telecomunicaciones	Interrupción puede colapsar coordinación de emergencias.	Redundancia de fibra. Protocolos de emergencia analógicos de respaldo.
Sistema de transporte (ADIF, puertos, aeropuertos)	Ataque puede paralizar logística nacional e internacional.	Certificación de seguridad obligatoria para todos los sistemas de gestión.

4. Los Cuatro Pilares del Modelo

4.1 Centro Nacional de Ciberseguridad reforzado

El INCIBE (Instituto Nacional de Ciberseguridad) y el CCN-CERT (del CNI) son los organismos actuales. El modelo propone su refuerzo y coordinación real:

- Centro de Operaciones de Seguridad (SOC) nacional con monitorización 24/7 de todas las infraestructuras criticas del Estado.
- Protocolo de respuesta a incidentes con tiempos máximos tasados: detección en menos de 1 hora, contención en menos de 4 horas, recuperación en menos de 24 horas para servicios críticos.
- Coordinación obligatoria entre el CNI, la Policía Nacional (Unidad de Investigación Tecnológica), la Guardia Civil (Grupo de Delitos Telemáticos) y el Mando Conjunto del Ciberespacio del Ejercito.
- Compartición obligatoria de información sobre amenazas entre administraciones publicas y operadores de infraestructuras criticas en tiempo real.

4.2 Protección del ciudadano digital

El ciudadano es el eslabón mas débil de la cadena de ciberseguridad y el objetivo mas frecuente del cibercriminal:

- Extensión del sistema de alertas de AUXILIA a amenazas digitales: avisos inmediatos sobre fraudes activos, phishing y estafas online en la zona geográfica o sector del ciudadano.
- Servicio gratuito de asesoramiento en ciberseguridad para ciudadanos victimas de fraude digital, integrado en las oficinas hibridas de protección ciudadana ya propuestas.
- Programa nacional de educación en ciberseguridad básica desde la educación secundaria: contraseñas seguras, identificación de phishing, protección de datos personales y uso seguro de redes sociales.
- Obligación de los bancos y plataformas de pago de reembolsar en menos de 48 horas los fraudes electrónicos acreditados cuando la entidad no ha implementado las medidas de seguridad reglamentarias.

4.3 Soberanía tecnológica y reducción de dependencias

España y Europa dependen excesivamente de tecnología de terceros países para sus sistemas críticos. Esa dependencia es una vulnerabilidad estratégica:

- Auditoria obligatoria de los sistemas tecnológicos utilizados en infraestructuras criticas para identificar componentes de países con riesgo geopolítico elevado.
- Plan de sustitución progresiva de tecnología critica dependiente de proveedores no europeos en sistemas de administración publica y defensa.
- Incentivos fiscales para empresas españolas y europeas que desarrollen alternativas tecnológicas soberanas en áreas criticas: comunicaciones cifradas, sistemas operativos seguros, hardware de red.
- Participación activa en los programas europeos de soberanía tecnológica: GAIA-X para cloud europeo, chip europeo y programas de IA soberana.
- Veto a tecnología de países considerados amenaza por el CNI en redes 5G y sistemas de comunicación de infraestructuras criticas.

4.4 Talento nacional en ciberseguridad

España tiene un déficit estructural de profesionales de ciberseguridad que no se resuelve sin una política activa:

- Programa nacional de becas en ciberseguridad vinculadas a compromiso de trabajo en administración publica o empresa estratégica española durante un mínimo de 3 anos.
- Especializaciones de FP en ciberseguridad (conectando con la reforma de FP ya propuesta) orientadas a perfiles técnicos de alta demanda: analistas de amenazas, técnicos de respuesta a incidentes, auditores de seguridad.
- Red de centros de excelencia en ciberseguridad en universidades españolas con financiación publica y colaboración con empresas del sector.
- Retención de talento: condiciones salariales competitivas para los especialistas en ciberseguridad del sector publico que eviten la fuga masiva hacia el sector privado o al extranjero.
- Programa de reservistas cibernéticos: profesionales del sector privado que en caso de ciberataque grave pueden ser movilizados para reforzar la respuesta nacional, similar al modelo finlandés.

5. Ciberseguridad de los Sistemas de España Eficiente

Todos los sistemas digitales propuestos en el modelo de España Eficiente deben nacer con ciberseguridad integrada desde el diseño, no añadida posteriormente:

Sistema de España Eficiente	Requisito de ciberseguridad
App GIF (gestión fiscal digital)	Cifrado extremo a extremo. Autenticación multifactorial obligatoria. Auditoria de seguridad semestral independiente.
App AUXILIA (alertas de emergencia)	Arquitectura recipiente ante ataques de denegación de servicio. Cifrado de geolocalización. Servidores en territorio nacional.
Sistema DVO (dispositivo de verdad objetiva)	Custodia judicial de los datos. Acceso restringido con trazabilidad total. Cifrado cuántico para datos mas sensibles.
Tarjeta sanitaria única nacional	Segmentación de acceso por rol profesional. Registro de cada acceso. Cumplimiento del Esquema Nacional de Seguridad nivel alto.
Dashboard de transparencia del gasto publico	Datos en lectura publica pero con escritura restringida y auditada. Protección ante manipulación de datos.
Oficinas hibridas de protección ciudadana	Comunicaciones cifradas. Protección de datos de victimas con nivel máximo. Aislamiento de sistemas de alerta infantil.

6. Marco Legal

Elemento	Marco legal
Protección de infraestructuras criticas	Ley 8/2011 de Protección de Infraestructuras Criticas. Real Decreto 704/2011.
Ciberseguridad nacional	Ley 36/2015 de Seguridad Nacional. Estrategia Nacional de Ciberseguridad.
Seguridad de sistemas de información públicos	Real Decreto 311/2022 del Esquema Nacional de Seguridad (ENS).
Ciberdefensa militar	Mando Conjunto del Ciberespacio (MCCE). Marco jurídico de las Fuerzas Armadas.
Marco europeo de ciberseguridad	Directiva NIS2 (UE 2022/2555). Reglamento de Ciberresiliencia de la UE. ENISA.
Protección de datos en sistemas críticos	RGPD (UE) 2016/679. LO 3/2018 LOPDGDD.
Cibercrimen	Convenio de Budapest sobre Ciberdelincuencia. Arts. 197 y ss. CP (delitos informáticos).

7. Indicadores de Evaluación

Indicador	Meta
Tiempo medio de detección de incidente en infraestructura critica	Menos de 1 hora en 3 años
Tiempo medio de recuperación de servicio critico tras ataque	Menos de 24 horas en 3 años
Porcentaje de sistemas críticos con certificación ENS nivel alto	100% en 5 años
Numero de especialistas en ciberseguridad en sector publico	Incremento del 50% en 5 años
Tasa de reembolso de fraudes digitales a ciudadanos en plazo	Superior al 90% en 3 años

8. Conclusión

La ciberseguridad no es un tema técnico para especialistas.
Es una cuestión de seguridad nacional, de soberanía y de confianza ciudadana.

Un hospital sin ciberseguridad es un hospital vulnerable.

Un sistema fiscal digital sin ciberseguridad es una trampa.
Una app de emergencias sin ciberseguridad es un riesgo para quien la usa.

España Eficiente digitaliza el Estado.
Y lo digitaliza con seguridad desde el primer día.
Porque la digitalización sin ciberseguridad no es modernización. Es vulnerabilidad.

Este Policy Brief forma parte de España Eficiente: El Modelo Completo.
Relacionado con: Sistema GIF y ROC | AUXILIA | DVO | Tarjeta Sanitaria Única | FP Dirigida al Empleo | Defensa Nacional.