Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ Instituto Nacional de Ciberseguridad

Diego Domínguez Martínez
presenta el resumen del trabajo

2024 Report on the state of cibersecurity in the union

European Union Agency for Cybersecurity (ENISA)

29 de enero de 2025

SERIE DE RESÚMENES EN ESPAÑOL

Palabras clave: Ciberseguridad, cadena de suministro, computación cuántica, CSIRTs (Equipos de Respuesta a Incidentes), Directiva NIS2, ENISA (Agencia Europea de Ciberseguridad), fakenews, Inteligencia Artificial, Internet de las Cosas, APTs (Amenazas persistentes avanzadas), ataques DDoS, ciberhigiene, phising, ransomware.

Introducción y Contexto

El *"2024 Report on the State of Cybersecurity in the Union"*, elaborado por la Agencia de Ciberseguridad de la Unión Europea (ENISA) en colaboración con la Comisión Europea y el Grupo de Cooperación NIS analiza el estado de la ciberseguridad en la Unión Europea.

El documento busca identificar las principales vulnerabilidades y desafíos actuales, así como proponer recomendaciones para mejorar la seguridad social de los Estados Miembros (MSs).

El informe resulta clave dado el contexto geopolítico en el que nos encontramos, marcado por la guerra en Ucrania, la creciente dependencia digital y el auge de la inteligencia artificial.

1. Marco legislativo

Visión general

En los últimos años la Unión Europea ha marcado la ciberseguridad como un área prioritaria, siendo este un campo que ha evolucionado enormemente en los últimos años. En esta sección se abordan las principales normativas que han llevado al panorama actual de los Estados Miembros.

1.1. Evolución del marco legal

- La **Directiva sobre la Seguridad de Redes y Sistemas de Información (NIS2)** es el principal componente legislativo que fija el marco de ciberseguridad en la Unión Europea.
- La **Ley de Resiliencia Cibernética (CRA)** establece estándares comunes de ciberseguridad de productos digitales desde su diseño hasta su mantenimiento. Algunos puntos clave recaen en gestionar vulnerabilidades durante todo el ciclo de vida del producto y la obligatoriedad de notificar vulenaribilidades e incidentes graves.
- La **Ley de Cibersolidaridad (CSOA)** busca fortalecer la capacidad de reacción de la Unión Europea frente a incidentes cibernéticos a gran escala. Incluye:
  1. Un sistema de alerta europeo para incidentes cibernéticos
  2. Un mecanismo de emergencia para

la coordinación de respuestas
3. Un mecanismo de revisión de incidentes críticos

- La **Enmienda al Acto de ciberseguridad** busca mejorar la capacidad de certificación en ciberseguridad en la UE.

1.2. Legislaciones sectoriales específicas

La UE también ha creado regulaciones para sectores particulares.

1. **Regulación DORA** (Ley de Resiliencia Operativa Digital). establece requisitos para garantizar la resiliencia digital y la gestión de riesgos en el sector financiero.
2. **Código de Red para la Electricidad**. Define reglas para abordar aspectos de ciberseguridad en los flujos eléctricos transfronterizos.
3. **Reglamento sobre Identidad Digital Europea** (EUDIF): Introduce un marco para la identidad digital segura, aspecto imprescindible para contar con servicios digitales confiables.

1.3. Relevancia del Marco Legal

El objetivo de las leyes de la UE es unificar la protección contra ciberataques en todos los países miembros, asegurando que trabajen juntos y de forma equilibrada. Aun así, algunos países tienen problemas para aplicar estas normas ya que no cuentan con los mismos recursos o experiencia. Este trabajo conjunto es fundamental para garantizar un nivel de seguridad similar en toda Europa.

1.4. Retos y Oportunidades

El marco legislativo de la UE, aun siendo uno de los más avanzados, plantea retos como el apoyo a los Estados Miembros que se retrasen en la implementación de las leyes, garantizar que las normativas no se solapen ni entren en conflicto, y la adpatación de las normativas a las nuevas tecnologías y a las amenazas emergentes.

En paralelo, estas normativas presentan oportunidades como la cooperación transfronteriza o el desarrollo de diversas capacidades.

2. Amenazas cibernéticas

En los últimos años, las amenazas cibernéticas se han incrementado, tanto en número como en complejidad. La Unión Europea enfrenta un entorno digital cada vez más vulnerable debido a factores como la digitalización acelerada y la interconexión global. A continuación, se enumeran las amenazas principales.

2.1. Ransomware y ataques DDoS

El ransomware y los ataques de denegación de servicio distribuido (DDoS) son los ataques más frecuentes en la UE. Estos ataques buscan extorsionar dinero bloqueando datos y saturando sistemas para interrumpir servicios esenciales, respectivamente. Ambos generan un gran impacto negativo tanto en empresas como en servicios públicos.

2.2. Ciberespionaje

El ciberespionaje sigue siendo una amenaza a día de hoy. Grupos vinculados a estados, como Rusia y China, han intensificado sus actividades en Europa. Estos actores suelen enfocarse en recopilar información estratégica de instituciones gubernamentales, empresas tecnológicas y sectores críticos.

2.3. Manipulación de información

La desinformación y la manipulación de información digital también han crecido. Estas técnicas se usan frecuentemente durante eventos importantes como elecciones, con el fin de influir en la opinión pública y generar inestabilidad. Tecnologías como la inteligencia artificial han facilitado la creación de contenido

falso y campañas de desinformación más sofisticadas.

2.4. Amenazas a la cadena de suministro

Los ataques a la cadena de suministro son un punto crítico dado que afectan a múltiples organizaciones comprometiendo un único proveedor. Estos ataques pueden ser difíciles de detectar y tienen el potencial de causar daños a gran escala

2.5. Uso de inteligencia artificial en cibercrimen

La inteligencia artificial se ha convertido en una herramienta muy útil, tanto para defenderse como para atacar. Los ciberdelincuentes la están utilizando para mejorar ataques como el phishing, crear contenidos falsos más convincentes y automatizar sus actividades maliciosas.

2.6. Panorama global

Conflictos geopolíticos como la guerra en Ucrania y las tensiones internacionales han aumentado el riesgo de ataques cibernéticos organizados. Estos ataques suelen ser parte de estrategias con múltiples pasos que combinan acciones digitales con sabotajes físicos o campañas de propaganda entre otros.

2.7. Preparación y respuesta

En respuesta al aumento de amenazas significativas, los países de la UE están mejorando su preparación. Esto incluye la cooperación entre Estados Miembros o el desarrollo de nuevas estrategias para detectar y responder a estos ataques. Los CSIRTs nacionales, que son equipos de respuesta a incidentes de seguridad informática también se están fortaleciendo, conocida la importancia de una reacción temprana ante este tipo de incidentes.

3. Capacidades de ciberseguridad a nivel Unión

La Unión Europea trabaja constantemente en la mejora de sus capacidades de ciberseguridad, asegurándose de que los Estados Miembros y sectores clave estén siempre preparados ante cualquier amenaza digital.

3.1. Hallazgos Generales

El informe evalúa las capacidades generales de la UE en el área de la ciberseguridad mediante el *EU Cybersecurity Index*, que mide factores como la prevención, la detección y la respuesta a incidentes. En 2024, la puntuación promedio fue de 62.65 sobre 100, todavía con margen de mejora en varios países.

3.2. Capacidades Nacionales

Cada Estado Miembro tiene su propia estrategia nacional de ciberseguridad y , aunque la mayoría están alineadas con los objetivos de la UE, otros países muestran discrepancias en áreas como el manejo de vulnerabilidades y notificación de incidentes o la investigación y desarrollo en ciberseguridad. Estas discrepancias deben solucionarse para mejorar la cooperación entre países.

3.3. Sector Privado

Los sectores críticos, como telecomunicaciones, finanzas y energía, muestran altos niveles de madurez en ciberseguridad. Sin embargo, otros sectores, como salud o transporte, enfrentan desafíos debido al uso de sistemas obsoletos difíciles de proteger o la falta de inversión en seguridad digital. Mejorar la colaboración entre entidades privadas y gobiernos es esencial para fortalecer estas áreas.

3.4. Concienciación y Ciberhigiene en la Sociedad

Aunque la mayoría de los ciudadanos europeos son más conscientes de los riesgos cibernéticos, casi la mitad carece de habilidades digitales básicas. Además, pocos conocen

los canales oficiales para reportar cibercrímenes. Es imprescindible continuar promoviendo la educación en ciberseguridad para reducir esta brecha.

3.5. Importancia de la Colaboración

La cooperación a nivel europeo, a través de redes como el *NIS Cooperation Group* y la Red de CSIRTs es clave para mejorar las capacidades colectivas. Estas iniciativas permiten compartir información, coordinar respuestas a incidentes y garantizar un enfoque uniforme en toda la Unión.

4. Gestión de crisis cibernéticas

La gestión de crisis cibernéticas es una parte esencial dentro de las capacidades de ciberseguridad a nivel de la Unión. En este apartado se recogen las estrategias y herramientas necesarias para prevenir, mitigar y responder a incidentes cibernéticos que puedan comprometer infraestructuras críticas, servicios esenciales o la seguridad nacional.

4.1. Monitoreo de amenazas

El monitoreo y la anticipación de amenazas en ciberseguridad son fundamentales para identificar, comprender y prevenir riesgos potenciales. Durante el periodo de análisis, los Estados Miembros han avanzado en la creación de sistemas nacionales de alerta temprana y en la integración de herramientas de monitoreo que permiten mejorar la detección y la respuesta ante incidentes cibernéticos. La cooperación entre los Centros Nacionales de Respuesta a Incidentes de Seguridad Informática (CSIRTs) y la red CSIRTs de la UE ha fortalecido el intercambio de información y la coordinación de actividades en casos de crisis.

4.2. Capacidades nacionales de los CSIRTs

Los CSIRTs desempeñan un papel crucial en la gestión de crisis cibernéticas. Sin embargo, se observó una variabilidad en su nivel de madurez y alineación con estándares internacionales. Aunque los CSIRTs están bien integrados en redes internacionales como *Trusted Introducer* y FIRST, el índice de madurez promedio a nivel de la Unión es de tan solo 10,31 sobre 100.

4.3. Ejercicios nacionales de ciberseguridad

El uso de ejercicios nacionales de ciberseguridad ha demostrado ser una herramienta efectiva para evaluar y fortalecer las capacidades de respuesta a incidentes. Durante el periodo de estudio, varios Estados Miembros llevaron a cabo simulacros enfocados en amenazas específicas, involucrando tanto a entidades públicas como privadas. Estos ejercicios permitieron identificar puntos débiles en la preparación, mejorar la coordinación entre instituciones y promover la colaboración en la gestión de crisis.

4.4. Recomendaciones clave

Para reforzar la gestión de crisis cibernéticas en la Unión, se propone:

1. Revisar y actualizar el Plan de Respuesta Coordinada ante Incidentes Cibernéticos a Gran Escala de la UE (**EU Blueprint**) para reflejar los últimos desarrollos en políticas de ciberseguridad.

2. Promover la adopción de estándares internacionales en los CSIRTs, así como su certificación para garantizar un nivel uniforme de madurez.

3. Fomentar la realización de ejercicios nacionales e internacionales regularmente, incluyendo situaciones más complejas que permitan evaluar la capacidad de respuesta conjunta.

4. Proveer de apoyo técnico y financiero a

los EM para el desarrollo de capacidades avanzadas de detección y respuesta.

El fortalecimiento de la gestión de crisis cibernéticas de la Unión Europea es fundamental para aumentar su resiliencia frente a un panorama de amenazas en constante evolución.

5. Seguridad de la cadena de suministro

La cadena de suministro es uno de los eslabones más vulnerables en el ámbito de la ciberseguridad. Esto se debe a su naturaleza compleja, donde múltiples proveedores, subcontratistas y servicios externos intervienen, creando una red extensa y difícil de supervisar. Un ataque dirigido a un solo proveedor puede tener consecuencias en cadena, afectando a varias organizaciones e incluso sectores enteros.

El informe destaca que los ataques a la cadena de suministro han aumentado significativamente, tanto en frecuencia como en sofisticación. Estos ataques suelen centrarse en vulnerabilidades dentro de productos o servicios, comprometiendo así a las empresas afectadas, sus socios y clientes.

Para enfrentar esta amenaza, se recomienda adoptar varias medidas clave:

1. **Establecer estándares comunes de seguridad:** Crear reglas claras y uniformes en toda la Unión Europea que aseguren que los proveedores de servicios críticos implementen buenas prácticas de ciberseguridad.

2. **Evaluaciones coordinadas de riesgos:** Realizar análisis periódicos de las cadenas de suministro para identificar posibles puntos débiles antes de que puedan ser explotados.

3. **Mayor transparencia:** Incentivar a los proveedores a compartir información sobre sus medidas de seguridad y vulnerabilidades detectadas, lo que permita a las empresas y gobiernos entender mejor los riesgos asociados.

Además, uno de los mayores desafíos que surgen en la cadena se suministro es la falta de visibilidad en las capas más profundas. Muchas organizaciones desconocen los proveedores secundarios o terciarios con los que trabajan sus socios, lo que dificulta prever y mitigar amenazas.

El uso de tecnologías avanzadas es también una prioridad. Soluciones como herramientas de monitoreo en tiempo real, inteligencia artificial y sistemas de detección de vulnerabilidades pueden ayudar a identificar problemas antes de que se conviertan en amenazas graves. Estas tecnologías, combinadas con auditorías regulares, pueden fortalecer significativamente la seguridad en las cadenas de suministro.

Por último, se resalta la importancia de mejorar la seguridad de la cadena de suministro, ya que esto no solo protege a las empresas, también fortalece la confianza de consumidores y socios comerciales en la Unión Europea. Esto resulta esencial en un mundo cada vez más globalizado e interconectado, donde los fallos en la seguridad pueden tener impactos a gran escala.

6. Habilidades en ciberseguridad

El desarrollo de habilidades en ciberseguridad es un elemento esencial para fortalecer la resiliencia digital en la Unión Europea. La constante evolución de las amenazas, sumada a la rápida digitalización de sectores críticos, requiere de un personal altamente capacitado capaz de anticipar, mitigar y responder a incidentes cibernéticos.

6.1. Brecha de habilidades en ciberseguridad

Uno de los principales desafíos en la UE es la brecha de habilidades en ciberseguridad. Actualmente, la demanda de profesionales supera ampliamente la oferta. Este déficit afecta tanto al ámbito público como privado, donde las organizaciones enfrentan dificultades para encontrar personal cualificado que cumpla con

las exigencias de los marcos legislativos como la Directiva NIS2.

Según datos recientes, más del 50 % de las entidades en la UE planean contratar nuevos especialistas en ciberseguridad durante los próximos dos años, pero el ritmo de incorporación no es suficiente para satisfacer la demanda. Este problema es especialmente agudo en las pequeñas y medianas empresas (PYMES), que a menudo carecen de los recursos necesarios para competir con grandes corporaciones en la atracción de talento.

6.2. Educación y formación en ciberseguridad

El sistema educativo y de formación juega un papel clave para abordar la brecha de habilidades. La mayoría de los Estados Miembros han introducido programas de grado y posgrado en ciberseguridad, así como certificaciones especializadas para formar profesionales en esta área.

ENISA, a través de iniciativas como el *European Cybersecurity Skills Framework* (ECSF) y la base de datos *CyberHEAD*, busca estandarizar las competencias en ciberseguridad y proporcionar una herramienta centralizada para que los ciudadanos puedan acceder a oportunidades de formación. Además, el programa *Cybersecurity Skills Academy*, parte del Año Europeo de las Competencias 2023, se ha propuesto cerrar la brecha de talento en la UE mediante estrategias que incluyan la formación, el reciclaje profesional (*reskilling*) y el perfeccionamiento (*upskilling*) de trabajadores en el sector.

6.3. Desafíos y oportunidades

Aunque se han logrado avances significativos, todavía existen desafíos importantes:

- **Falta de formación especializada:** Muchas universidades y centros educativos no cuentan con programas específicos en ciberseguridad o con los recursos necesarios para ofrecer formación práctica de calidad.
- **Heterogeneidad en los estándares:** Hay una gran diferencia entre las competencias requeridas entre sectores y países, dificultando la movilidad y el reconocimiento de habilidades a nivel europeo.
- **Falta de inclusión:** Grupos subrepresentados, como las mujeres y las personas de áreas rurales, enfrentan barreras para acceder a la educación y las oportunidades laborales en ciberseguridad.

A pesar de estos retos, existen otras oportunidades:

- **Colaboración público-privada:** Las empresas pueden asociarse con instituciones educativas para diseñar programas que respondan a las necesidades del mercado.
- **Programas de mentoría:** La creación de mentorías y apoyo pueden ayudar a retener y desarrollar talento en ciberseguridad.
- **Uso de tecnologías innovadoras:** Simuladores, entornos de aprendizaje gamificados y plataformas en línea pueden complementar la formación tradicional y llegar a una audiencia más amplia.

6.4. Recomendaciones para fortalecer las habilidades en ciberseguridad

Para abordar estas brechas se proponen las siguientes acciones:

1. Ampliar la financiación y el apoyo a programas educativos en ciberseguridad.
2. Promover la igualdad de acceso a la formación.
3. Implementar un sistema europeo de certificación de competencias en ciberseguridad para facilitar el reconocimiento mutuo entre los Estados Miembros.
4. Fomentar la formación continua y el reciclaje profesional para garantizar que los trabajadores puedan adaptarse a las nuevas tecnologías y amenazas emergentes.

El desarrollo de habilidades en ciberseguridad no solo fortalece la protección de la infraestructura digital de la UE, sino que también impulsa la competitividad y la innovación.

7. Ciberhigiene social

La concienciación y la ciberhigiene social representan pilares clave para fortalecer la resiliencia digital de la Unión Europea. La digitalización creciente de los servicios y la vida cotidiana ha expuesto a los ciudadanos a un panorama de amenazas más amplio y complejo, destacando la importancia de la educación y la adopción de prácticas seguras en línea.

El término *ciberhigiene social* se refiere al conjunto de prácticas, hábitos y comportamientos que los individuos y colectivos adoptan para minimizar los riesgos y proteger su información personal. Incluye actividades como el uso de contraseñas robustas, la actualización regular de software, la configuración adecuada de dispositivos, el manejo cuidadoso de datos personales y la prevención frente a intentos de suplantación de identidad (*phishing*).

A nivel social, la ciberhigiene busca crear una población informada y consciente de que las buenas prácticas digitales no solo reduce su propia vulnerabilidad, también contribuye a un ecosistema digital más seguro para todos.

7.1. Concienciación en la UE

Aunque ha habido avances en la sensibilización sobre ciberseguridad, aún hay brechas significativas en el conocimiento y la adopción de buenas prácticas entre la población. Según datos recientes, más del 45 % de los europeos carecen de habilidades digitales básicas, lo que limita su capacidad para protegerse en el entorno en línea. Por otro lado, el 93 % de los usuarios han cambiado la forma en que utilizan Internet debido a preocupaciones sobre seguridad, lo que refleja un creciente nivel de conciencia. Sin embargo, solo el 22 % de los ciudadanos están al tanto de los canales oficiales para reportar cibercrímenes, lo que resalta la importancia de dar a conocer los mecanismos de comunicación y apoyo en caso de incidentes.

7.2. Educación superior en ciberseguridad

La educación superior en ciberseguridad desempeña un papel crucial en la formación de profesionales capacitados para enfrentar los retos del entorno digital. Más de dos tercios de los Estados Miembros ofrecen programas de grado y posgrado en ciberseguridad. Sin embargo, existen discrepancias significativas en la disponibilidad y accesibilidad de estos programas.

Algunas iniciativas, como la *European Cybersecurity Skills Framework* (ECSF) y la base de datos *CyberHEAD*, impulsadas por ENISA, buscan estandarizar las competencias y facilitar el acceso a recursos educativos en ciberseguridad. Además, se han implementado programas de financiación en varios EM para fomentar el interés en esta área.

7.3. Iniciativas y recomendaciones

Para promover la concienciación y mejorar la ciberhigiene social, se propone:

1. Incluir programas de educación en ciberseguridad desde niveles primarios hasta superiores, adaptados a las necesidades de cada grupo demográfico.

2. Fomentar campañas de sensibilización a nivel nacional y europeo que utilicen medios accesibles y efectivos.

3. Promover la participación activa de empresas y organizaciones en la formación de sus empleados en prácticas seguras en línea.

4. Fortalecer los canales oficiales de reporte de incidentes cibernéticos y asegurarse de que sean ampliamente conocidos y accesibles para todos los ciudadanos.

5. Aumentar la colaboración entre los EM para estandarizar y expandir la oferta de programas educativos en ciberseguridad.

8. Proyecciones futuras

El futuro de la ciberseguridad en la Unión Europea es una incógnita difícil de resolver ante un panorama tecnológico en constante evolución. En este apartado se exploran las tendencias emergentes y los desafíos clave identificados en el informe, incluyendo el impacto de tecnologías revolucionarias como la inteligencia artificial y la computación cuántica.

8.1. IA maliciosa

La inteligencia artificial está transformando muchos sectores, pero también permite un mayor alcance de las amenazas cibernéticas. Los actores maliciosos están utilizando herramientas basadas en IA para automatizar ataques, generar contenido falso (como *deepfakes*) y diseñar campañas de desinformación más sofisticadas. Además, los modelos avanzados de IA pueden ser empleados para descubrir vulnerabilidades en sistemas de manera más rápida y precisa, aumentando el riesgo de explotación.

Por otro lado, la IA también permite para reforzar la ciberseguridad. Herramientas inteligentes pueden ayudar a detectar patrones de ataque en tiempo real, predecir amenazas y responder a incidentes de manera automatizada. El desarrollo y uso ético de estas tecnologías será crucial para garantizar que la IA sea una herramienta de defensa más que de ataque.

8.2. Computación cuántica

La computación cuántica representa una revolución tecnológica con implicaciones significativas para la ciberseguridad. Aunque aún está en desarrollo, los avances en esta tecnología podrían comprometer los sistemas de cifrado actuales, ya que los ordenadores cuánticos tienen el potencial de resolver problemas que serían inpensables para las computadoras clásicas.

La UE ha comenzado a prepararse para este desafío mediante el desarrollo de algoritmos resistentes a la computación cuántica. Estas soluciones, conocidas como criptografía postcuántica, buscan garantizar la seguridad de la información incluso en un futuro donde los sistemas de cifrado convencionales puedan quedar obsoletos.

8.3. Dependencia tecnológica y riesgos de interconectividad

La creciente dependencia de tecnologías digitales y la interconexión de sistemas críticos aumentan la superficie de ataque. Sectores como la energía, el transporte y la salud dependen cada vez más de sistemas interconectados, lo que introduce riesgos adicionales en caso de interrupciones o ataques dirigidos. Las proyecciones indican que estos sectores serán objetivos prioritarios de los actores maliciosos en los próximos años.

8.4. Escasez de habilidades y talento

Conforme aumenta la complejidad de las amenazas, la demanda de talento especializado en ciberseguridad continuará creciendo. La falta de profesionales cualificados podría limitar la capacidad de la UE para responder a incidentes y proteger sus infraestructuras críticas. Las iniciativas actuales, como la *Cybersecurity Skills Academy*, serán fundamentales para dotar de estas habilidades al personal necesario.

8.5. Recomendaciones estratégicas para el futuro

Para enfrentar estos desafíos emergentes, se proponen las siguientes estrategias:

- **Fomentar la investigación en tecnologías emergentes:** Invertir en el desarrollo de IA ética y criptografía postcuántica para adelantarse a las amenazas futuras.
- **Refuerzo de la colaboración internacional:** La naturaleza global de las amenazas cibernéticas requiere una mayor cooperación entre países para compartir información, recursos y mejores prácticas.

- **Desarrollo de normativas adaptativas:** Crear marcos legislativos que puedan adaptarse rápidamente para abordar los riesgos asociados a tecnologías emergentes.
- **Fortalecer las capacidades de predicción:** Implementar modelos avanzados de monitoreo y análisis para prever tendencias y anticiparse a los riesgos antes de que se materialicen.
- **Promover la resiliencia cibernética:** Fomentar la adopción de prácticas de ciberhigiene, fortalecer infraestructuras críticas y desarrollar estrategias de respuesta rápida ante incidentes.

El enfoque en estas áreas permitirá a la UE mantenerse a la vanguardia en la lucha contra amenazas cibernéticas, asegurando un entorno digital seguro y resistente que pueda adaptarse a las demandas del futuro.

9. Recomendaciones Políticas

El informe sugiere varias acciones clave para fortalecer la ciberseguridad en la Unión Europea, empezando por apoyar la implementación de normativas como la Directiva NIS2, brindando asistencia técnica y financiera a los países con menos recursos. También se recomienda reforzar las capacidades nacionales mediante la formación de equipos de respuesta (CSIRTs) y simulacros regulares.

Además, es fundamental mejorar la concienciación y la educación en ciberseguridad, incluyendo programas de formación para ciudadanos, empresas y estudiantes. Se destaca la importancia de proteger las cadenas de suministro con estándares comunes y evaluaciones de riesgos a nivel europeo.

Por último, se proponen mayores inversiones en tecnologías avanzadas como la inteligencia artificial y la computación cuántica, así como una mayor cooperación internacional para compartir información y coordinar respuestas ante amenazas globales.

10. Reflexión

Tras leer el informe, lo que más me ha llamado la atención es la importancia del factor humano en la ciberseguridad. Aunque hablamos de sistemas avanzados, inteligencia artificial y computación cuántica, al final todo tiene un componente humano. Me sorprendió especialmente el hecho de que casi la mitad de los ciudadanos de la Unión Europea no tienen habilidades digitales básicas. Esto no solo los hace más vulnerables a los riesgos en línea, también afecta la seguridad todos.

Otro punto que me sorprendió es cómo los sectores críticos, como la salud y el transporte, están cada vez más interconectados, lo que supone una gran ventaja en muchos aspectos, pero también los convierte en objetivos más atractivos para los ciberdelincuentes. Además, la brecha de habilidades en ciberseguridad es alarmante, necesitamos más profesionales preparados para enfrentar estas amenazas.

En resumen, me quedo con la idea de que la ciberseguridad no solo trata de tecnología, sino de educación, colaboración y responsabilidad a partes iguales. Todos jugamos un papel fundamental en hacer del entorno digital un lugar más seguro, desde el gobierno hasta las personas de “a pie”.

Referencias

· European Union Agency for Cibersecurity, *Report on the state of the art of cibersecurity* (13 de diciembre de 2024). DOI 10.2824/0401593, ISBN 978-92-9204-681-1