Contact Committee

Comité de contacto

de las Entidades Fiscalizadoras Superiores de la Unión Europea

Compendio de auditorías

La ciberseguridad en la UE y sus Estados miembros

Auditoría de la resiliencia de los sistemas de información y las infraestructuras digitales esenciales ante los ciberataques

Informes de auditoría
publicados entre 2014 y 2020

ES

Diciembre de 2020

El Comité de Contacto de las Entidades Fiscalizadoras Superiores (EFS) de la Unión Europea (UE) ofrece un foro para debatir y abordar cuestiones de auditoría pública de la UE. Aumentando el diálogo y la cooperación entre sus miembros, el Comité ayuda a incrementar la eficacia de la auditoría externa de las políticas y los programas de la UE. También contribuye a fomentar la rendición de cuentas, mejorar la gestión financiera de la UE y consolidar una buena gobernanza, en beneficio de todos los ciudadanos de la Unión.

Contacto: www.contactcommittee.eu

Índice

Página

Prólogo

Estimado lector:

La digitalización y el creciente uso de la tecnología de la información en todos los aspectos de nuestras vidas cotidianas están dando paso a un nuevo mundo de oportunidades. Sin embargo, también han acarreado un mayor riesgo de que las personas, las empresas y las autoridades públicas sean víctimas de la ciberdelincuencia o de un ciberataque, con el consiguiente agravamiento de sus repercusiones sociales y económicas.

Aunque la ciberseguridad sea una prerrogativa de los Estados miembros en la UE, esta desempeña una importante función al crear un marco normativo común dentro del mercado único de la UE y generar las condiciones para que los Estados miembros trabajen conjuntamente en un clima de confianza mutua.

La ciberseguridad y nuestra autonomía digital se han convertido en una cuestión de importancia estratégica para la UE y sus Estados miembros. En los sectores público y privado de todos los Estados miembros existen numerosas deficiencias en la gobernanza de la ciberseguridad, aunque a diferentes niveles. Esto menoscaba nuestra capacidad para limitar los ciberataques y, llegado el caso, responder ante los mismos. La desinformación, a menudo orquestada desde fuera de la UE, va en aumento, como se ha hecho patente de nuevo durante la pandemia de COVID-19 de este año. Esto supone una amenaza para la cohesión social en nuestras sociedades y para la confianza de los ciudadanos en nuestros sistemas democráticos que no podemos ignorar.

En 2018, una encuesta de las Entidades Fiscalizadoras Superiores (EFS) en la UE demostró que hasta ese momento alrededor de la mitad no había auditado la ciberseguridad. Desde entonces, nuestras EFS han dispuesto sus actividades de auditoría en materia de ciberseguridad, con especial atención a la protección de datos, la preparación de los sistemas contra los ciberataques y la protección de los sistemas de las empresas de servicios públicos esenciales. Como es comprensible, no todas estas auditorías pueden hacerse públicas, puesto que pueden contener información sensible de seguridad nacional.

Durante este año, la crisis del COVID-19 ha puesto a prueba el tejido económico y social de nuestras sociedades. Habida cuenta de nuestra dependencia de la tecnología de la información, la próxima pandemia bien podría ser una «cibercrisis». Hemos de estar preparados e incrementar la resiliencia de los sistemas de información e infraestructuras digitales esenciales contra los ciberataques.

Esperamos que el planteamiento general ofrecido en este compendio estimule el interés de los auditores públicos de toda la Unión en este ámbito crítico.

Klaus-Heiner Lehne

Presidente del Tribunal de Cuentas Europeo
Presidente del Comité de Contacto
y jefe del proyecto

Resumen

I La ciberseguridad y nuestra autonomía digital se han convertido en una **cuestión de importancia estratégica para la UE y sus Estados miembros**, por lo que, con el aumento del nivel de las amenazas, hemos de redoblar nuestros esfuerzos por proteger nuestros sistemas de información y nuestras infraestructuras digitales esenciales contra los ciberataques. La ciberseguridad no atañe únicamente a nuestros servicios públicos, sanitarios o de defensa, sino que también afecta a la protección de nuestros datos personales, modelos de negocio y propiedad intelectual. En definitiva, la ciberseguridad versa sobre proteger nuestras sociedades democráticas, nuestra independencia como europeos y la manera en que convivimos.

II En la primera parte de este tercer compendio del Comité de Contacto se expone **qué comporta la ciberseguridad**. En ella se describe por qué la ciberseguridad supone un desafío para las autoridades públicas, las empresas y las personas y se destaca el nuevo fenómeno de la desinformación, que constituye una creciente amenaza para la cohesión social en nuestras sociedades y sistemas democráticos. También se explican las competencias y los agentes de la UE en la materia, así como su estrategia y legislación y la financiación de la Unión disponible.

III En la segunda parte del compendio se resumen los **resultados de una selección de auditorías llevadas a cabo por veinte EFS de Estados miembros participantes y por el Tribunal de Cuentas Europeo**, publicadas entre 2014 y 2020. Dichas auditorías abordaron importantes aspectos de la ciberseguridad, como la protección de los datos privados, la integridad de los centros de datos nacionales, la seguridad de las instalaciones de las empresas de servicios públicos y la aplicación de estrategias de ciberseguridad nacionales, en un sentido amplio.

IV La tercera parte del compendio contiene **fichas informativas detalladas de las auditorías seleccionadas**, junto con una sinopsis de otras auditorías en materia de ciberseguridad publicadas por las EFS.

PARTE I – La ciberseguridad en el contexto europeo

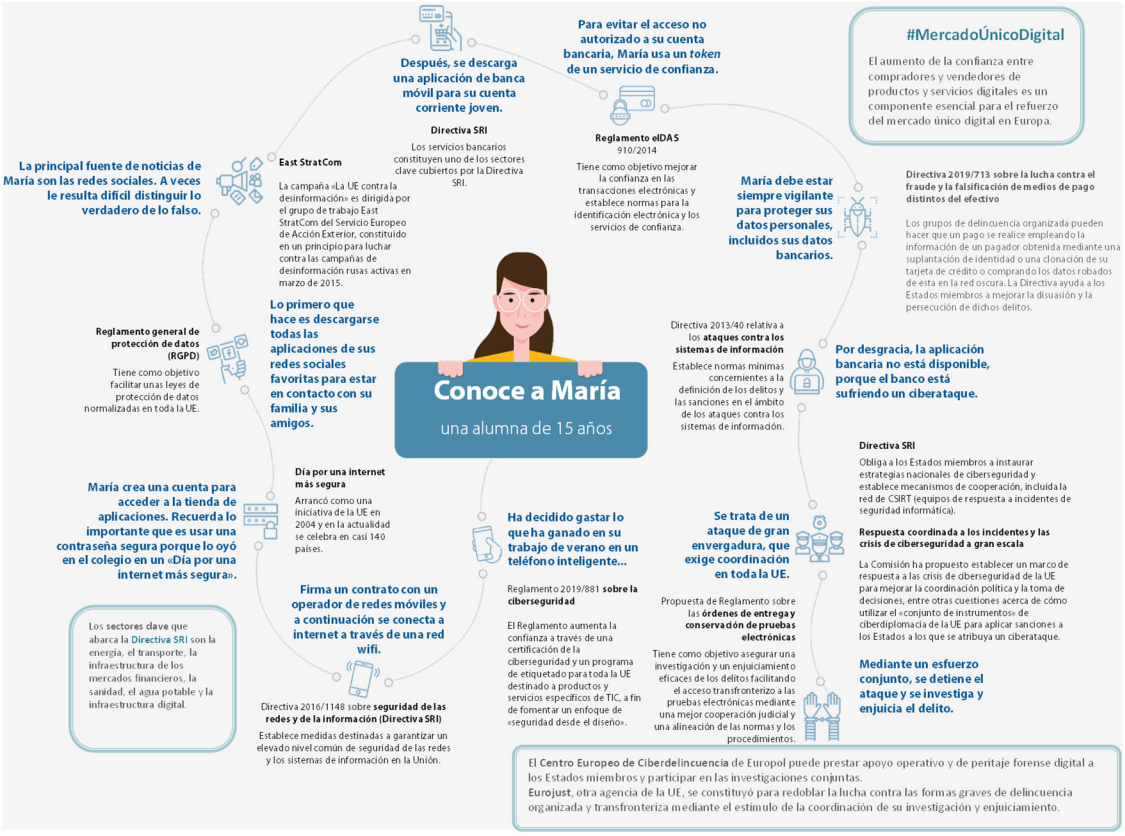
¿Qué es la ciberseguridad?

1 No existe ninguna **definición** normalizada y universal **de la ciberseguridad**. En el presente documento, por ciberseguridad se entienden **todas las actividades necesarias para la protección de las redes y los sistemas de información, los usuarios de tales sistemas y otras personas afectadas por ciberamenazas**. Consiste en prevenir y detectar ciberincidentes, así como responder ante los mismos y recuperarse de ellos. Dichos incidentes pueden ser intencionados o no y oscilar entre una divulgación accidental de información y ataques a empresas e infraestructuras críticas, el robo de datos personales o incluso la injerencia en procesos democráticos y electorales, pasando por las campañas generales de desinformación para influir en el debate público.

La ciberseguridad afecta a las vidas cotidianas de todos los ciudadanos de la UE

2 La ciberseguridad afecta a las vidas cotidianas de todos los ciudadanos de la UE cada vez que utilizan dispositivos tecnológicos personales, como teléfonos inteligentes o redes wifi, o los servicios de redes sociales o banca electrónica. Más que nunca, en 2020 ya no es cuestión de saber si un ciberataque tendrá lugar, sino cómo y dónde lo hará. Esta amenaza se cierne sobre todos nosotros: **personas, empresas y autoridades públicas**. En la ***imagen 1*** se muestra cómo la UE apoya la ciberseguridad y ha creado un marco para proteger de los ciberataques las actividades electrónicas cotidianas de los ciudadanos. Defender los sistemas de información y las infraestructuras digitales esenciales contra los ciberataques se ha convertido en un reto estratégico.

Imagen 1. Apoyo de la ciberseguridad por parte de la UE en la vida cotidiana de sus ciudadanos



Fuente: Tribunal de Cuentas Europeo, iconos creados por Pixel perfect de www.flaticon.com

Existen numerosos tipos de amenazas a la ciberseguridad

3 Los múltiples tipos de amenazas a la ciberseguridad a los que se enfrentan nuestras sociedades se pueden clasificar en función de **cómo afectan a los datos (divulgación, modificación, destrucción o negación de acceso)** o con arreglo a los principios fundamentales de seguridad de la información que vulneran (véase la ***ilustración 1***).

Ilustración 1. Tipos de amenazas y principios de la seguridad de la información que ponen en peligro

Candado = no afecta a la seguridad; Signo de exclamación = pone en peligro la seguridad

Fuente: Tribunal de Cuentas Europeo, a partir de un estudio del Parlamento Europeo[1].

4 Cada vez que un dispositivo se conecta a internet o a otros dispositivos, aumenta la denominada «superficie de ataque» de la ciberseguridad. El crecimiento exponencial del internet de las cosas, la nube, los macrodatos y la digitalización de la industria ha venido acompañado de un aumento de la exposición a las vulnerabilidades, lo que facilita a los atacantes llegar a cada vez más víctimas. La variedad de tipos de ataques y su creciente sofisticación hacen que sea difícil seguir el ritmo[2]. En el ***recuadro 1*** se describen ejemplos de **posibles ciberataques**.

---

[1] Parlamento Europeo, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, estudio para la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, septiembre de 2015.

[2] ENISA, *ENISA Threat Landscape Report 2017*, 18 de enero de 2018.

Recuadro 1

Tipos de ciberataques

Los **programas maliciosos** (programas informáticos malintencionados) están diseñados para dañar los dispositivos o las redes. Pueden contener virus, troyanos, programas de secuestro, gusanos, *adware* y programas espía (por ejemplo, NotPetya).

Los **programas de secuestro** encriptan datos e impiden a los usuarios acceder a sus archivos hasta que paguen un rescate, generalmente en una criptomoneda, o lleven a cabo una determinada acción. Según Europol, los ataques con programas de secuestro son los más frecuentes y en los últimos años se han multiplicado exponencialmente sus distintos tipos (por ejemplo, Wannacry[3]).

También están aumentando los ataques de **denegación de servicio distribuido** (DDoS), que impiden el acceso a los servicios o los recursos al inundarlos de más solicitudes de las que pueden gestionar; un tercio de las organizaciones se enfrentó a este tipo de ataque en 2017[4].

Los **ataques basados en la web** son un atractivo método mediante el cual los autores de las amenazas pueden engañar a las víctimas empleando sistemas y servicios web como vectores. Así abarcan una extensa vía de ataque, por ejemplo, utilizando URL o *scripts* malintencionados para dirigir al usuario o a la víctima al sitio web deseado o hacer que descarguen contenido malintencionado (ataques de abrevadero, descargas ocultas) e **insertando** código malicioso en un sitio web legítimo pero comprometido para robar información (*formjacking*) y utilizarla o venderla, obteniendo así un lucro ilegítimo[5].

Los usuarios pueden ser manipulados para que realicen una acción o desvelen información confidencial sin darse cuenta. Esta artimaña se puede utilizar para el robo de datos o para el ciberespionaje, y se conoce como **ingeniería social**. Hay distintas formas de conseguirlo, pero un método común es la **suplantación de identidad**, que consiste en engañar a los usuarios a través de correos que parecen procedentes de fuentes fiables para que revelen información o para que pulsen enlaces que infectarán los dispositivos con programas maliciosos descargados. Más de la mitad de los Estados miembros informaron de investigaciones de dichos ataques en redes[6].

Probablemente, el tipo de amenaza más perverso sean las **amenazas persistentes avanzadas**. Estas provienen de atacantes sofisticados que realizan una vigilancia a largo plazo y roban datos, en ocasiones con fines destructivos. Su objetivo es pasar desapercibidos durante el mayor tiempo posible. Las amenazas persistentes avanzadas están relacionadas a menudo con los Estados y tienen como objetivo

sectores especialmente delicados, como la tecnología, la defensa y las infraestructuras críticas. Se calcula que este tipo de **ciberespionaje** supone al menos una cuarta parte de todos los ciberincidentes[7].

El impacto económico de los ciberataques es significativo

5 En los últimos años, la amenaza de **los ciberataques y la ciberdelincuencia** se ha convertido en un gran problema. Ya en 2016, el 80 % de las empresas de la UE había sufrido al menos un incidente de ciberseguridad[8]. En 2018, el 40 % de los encuestados de organizaciones que empleaban la robótica o la automatización declaró que la interrupción de sus operaciones sería la consecuencia más grave de un ciberataque contra sus sistemas. Sin embargo, a pesar del conocimiento sobre los riesgos cibernéticos de perturbaciones, a menudo las empresas no tienen instalado un sistema para gestionarlos[9].

6 Desde entonces, el número de ciberataques, así como su gravedad y sus costes económicos, no han hecho más que crecer. En la medida en que se pueden calcular las **consecuencias financieras** de la ciberdelincuencia, esta le costará a la economía mundial **6 billones de dólares estadounidenses al año en 2021**, o sea, el doble de los 3

---

[3] El programa de secuestro *Wannacry* explotó las vulnerabilidades de un protocolo de Microsoft Windows que permite el control remoto de cualquier ordenador. Microsoft publicó un parche cuando descubrió la vulnerabilidad. Sin embargo, cientos de miles de ordenadores no habían sido actualizados y muchos resultaron infectados posteriormente. *Fuente:* A. Greenberg, «*Hold North Korea Accountable For Wannacry—and the NSA, too*», WIRED, 19 de diciembre de 2017.

[4] Europol, *Internet Organised Crime Threat Assessment 2018*.

[5] ENISA, *ENISA Threat Landscape 2020 – Web-based attacks*, 20 de octubre de 2020.

[6] Europol, véase lo que antecede, 2018.

[7] Centro Europeo de Economía Política Internacional, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, Occasional Paper n.º 2/18, febrero de 2018.

[8] Europol, *Internet Organised Crime Threat Assessment 2017*.

[9] PWC, Global State of Information Security (GSISS) *Survey – Strengthening digital society against cyber shocks*, 2017.

billones estimados en 2015[10]. Esta cifra se puede comparar con la estimación del PIB mundial en 2020 de 138 billones de dólares estadounidenses. Los costes de la ciberdelincuencia dimanan de los daños y la destrucción de datos, de la sustracción de capitales, de la pérdida de productividad, del robo de propiedad intelectual y de datos personales y financieros y del restablecimiento de la actividad ordinaria de las empresas, así como del daño a la reputación. La Junta Europea de Riesgo Sistémico (JERS) calcula que el coste medio de los ciberincidentes aumentó un 72 % entre 2015 y 2020[11].

7 La ciberdelincuencia **incide de manera diferente en los diversos sectores económicos**, según revela un reciente estudio de 2020[12]: fue el fenómeno de fraude más perturbador en el Gobierno y la Administración pública, el sector tecnológico, el de los medios de comunicación y de las telecomunicaciones y en el sector sanitario (véase el ***recuadro 2***); también fue el segundo problema con mayor efecto perturbador en los sectores financiero, industrial y manufacturero.

[10] Cybersecurity Ventures, *2019 Official Annual Cybercrime Report*, patrocinado por Herjavec Group, 2019.

[11] JERS, Junta Europea de Riesgo Sistémico, *Systemic cyber risk*, febrero de 2020.

[12] PWC, *Fighting fraud: A never-ending battle PwC's Global Economic Crime and Fraud Survey*, 2020.

Recuadro 2

Chantaje a pacientes de psicoterapia finlandeses con datos médicos personales robados entre 2018 y 2019

En 2020, algunos pacientes de una gran clínica de psicoterapia finlandesa con delegaciones en todo el país fueron contactados individualmente por un chantajista, después de que robara sus datos personales en noviembre de 2018, con una posible violación de la seguridad adicional en marzo de 2019. Por lo que parece, los datos contenían información de identificación personal y notas sobre lo hablado en las sesiones de terapia.

El chantaje consistía en que si la clínica y los pacientes no abonaban al delincuente una suma en *bitcoins*, se publicarían los datos. El incidente dio lugar a que el Gobierno finlandés celebrara una reunión de emergencia[13].

8 En 2019, Europol[14] destacó nuevamente **la persistencia y la tenacidad de una serie de amenazas clave de ciberdelitos**:

- los ataques con programas de secuestro siguen siendo la principal amenaza, ya que se orientan con cada vez mayor precisión y su rentabilidad —así como los daños ocasionados— no hace más que aumentar. Mientras los programas de secuestro supongan una fuente de ingresos relativamente sencilla para los ciberdelincuentes y sigan ocasionando pérdidas económicas y daños significativos, es probable que continúen en lo más alto del podio de las amenazas por ciberdelincuencia;
- la suplantación de identidad y los protocolos de escritorio remoto vulnerables suponen los principales vectores de infección por programas maliciosos;
- los datos siguen siendo un objetivo, una mercancía y un catalizador clave de la ciberdelincuencia.

[13] BBC News, *Therapy patients blackmailed for cash after clinic data breach*, 26 de octubre de 2020.

[14] Europol, *INTERNET organised crime threat assessment (IOCTA)*, 2019.

9 De manera similar, en su **informe de 2020 *Main incidents in the EU and worldwide***[15], la Agencia de la Unión Europea para la Ciberseguridad (ENISA) ofrece una serie de ejemplos de incidentes de ciberseguridad (véase el ***recuadro 3***).

Recuadro 3

Agencia de la Unión Europea para la Ciberseguridad (ENISA): incidentes de ciberseguridad 2019-2020

La plataforma de correo electrónico verifications.io sufrió una importante violación de la seguridad de los datos debido a MongoDB, una base de datos desprotegida. Quedaron expuestos más de 800 millones de correos electrónicos con información sensible, entre la que se contaba información de identificación personal (PII, por sus siglas en inglés).

En un popular foro de pirateo informático alojado por el servicio en la nube MEGA1 se publicaron 770 millones de direcciones de correo electrónico y 21 millones de contraseñas únicas. Pasó así a convertirse en «Collection #1», el mayor conjunto de credenciales personales robadas de la historia.

Citrix, el proveedor de servicios de virtualización y en la nube, fue víctima de un ciberataque específicamente dirigido contra él. Para abrirse paso hasta los sistemas de Citrix, los atacantes aprovecharon varias vulnerabilidades informáticas críticas, como CVE-2019-19781, y emplearon una técnica denominada *password spraying*.

El proveedor de alojamiento en la nube iNSYNQ19 sufrió un ataque con un programa de secuestro que imposibilitó el acceso de los clientes a sus datos durante más de una semana, viéndose obligados a recurrir a sus copias de seguridad locales.

10 Según Europol, los ciberataques diseñados para causar unos **daños duraderos** se duplicaron durante los primeros seis meses de 2019, principalmente en el sector manufacturero. A diferencia de los ataques con programas de secuestro «convencionales», se trata de actos de sabotaje que borran permanentemente o en cualquier caso dañan de manera irreversible los datos empresariales (véase el ***recuadro 4***).

---

[15] ENISA, *Main incidents in the EU and worldwide – From January 2019 to April 2020*, octubre de 2020.

Recuadro 4

Programas de secuestro destructivos: los ataques de Germanwiper en 2019

En 2019, se detectó una serie de ataques con programas de secuestro dirigidos contra empresas que operaban en Alemania. Apodado *Germanwiper*, el programa de secuestro en cuestión podía sustituir los archivos infectados por ceros y unos, imposibilitando así su recuperación. Este programa se difundió a través de campañas de suplantación de identidad por correo electrónico e iba dirigido en particular contra el personal de recursos humanos de grandes empresas, ya que iba incorporado en solicitudes de empleo falsas[16].

La sensibilización sobre las amenazas a la ciberseguridad está aumentando a la par que su frecuencia

11 Sin embargo, hasta hace poco, la sensibilización y el reconocimiento sobre dichos riesgos se situaban en niveles bastante bajos. En 2017, el 69 % de las empresas de la UE tenía un conocimiento nulo o básico de su **exposición a las amenazas cibernéticas**[17] y el 60 % no había calculado nunca las **potenciales pérdidas económicas**[18]. Además, según una encuesta mundial de 2018, un tercio de las organizaciones preferiría pagar el rescate al pirata informático en vez de invertir en seguridad de la información[19].

---

[16] Cybersecurity Insiders, *GermanWiper Ransomware attack warning for Germany*, sin fecha.

[17] Comisión Europea, *Ficha informativa sobre la ciberseguridad*, septiembre de 2017.

[18] Entre dichas pérdidas cabe citar la pérdida de ingresos, los gastos de reparación de sistemas dañados, las posibles responsabilidades por activos o información robados, los incentivos de retención de clientes, unas primas de seguros más altas, el incremento de los costes de protección (nuevos sistemas, trabajadores, formación, etc.) y las posibles liquidaciones de gastos de cumplimiento o litigios.

[19] NTT Security, *Risk: Value 2018 Report*.

12 En el **Eurobarómetro de 2020 sobre la actitud de los europeos frente a la ciberseguridad**[20] se determina la creciente sensibilización —y preocupación— de los ciudadanos de la UE:

- a los usuarios de internet encuestados les inquieta sobre todo que alguien realice un uso indebido de sus datos personales (46 %), la seguridad de sus pagos en línea (41 %), no poder inspeccionar artículos o pedirle asesoramiento a una persona real, o no recibir los artículos o los servicios adquiridos en línea (ambos el 22 %);
- más de tres cuartas partes (76 %) de los encuestados creen que el riesgo de ser víctima de un ciberdelito está aumentando. Sin embargo, muchos menos (el 52 %) creen que pueden protegerse suficientemente al respecto, lo que supone un descenso de nueve puntos porcentuales con respecto a 2018;
- poco más de la mitad de los encuestados (el 52 %) creen que están bien informados sobre la ciberdelincuencia, pero solo el 11 % dice sentirse muy bien informado.

La ciberseguridad es importante para la cohesión social y la estabilidad política

Una nueva amenaza: ciberseguridad y desinformación

13 La difusión deliberada, sistemática y a gran escala de **desinformación constituye un enorme reto estratégico para nuestras democracias**[21]. La desinformación y las noticias falsas tienen el potencial de dividir a las sociedades, sembrar recelos e incluso socavar la cohesión social y la confianza en los procesos democráticos (véase el ***recuadro 5***).

---

[20] Comisión Europea, *Special Eurobarometer 499 – Europeans' attitudes towards cyber security*, enero de 2020.

[21] Con arreglo al estudio *The Global Disinformation Order*, publicado por la Universidad de Oxford en septiembre de 2019, el número de países con campañas políticas de desinformación ha aumentado considerablemente hasta alcanzar los 70 en los últimos dos años.

Recuadro 5

Desinformación

La Comisión Europea define la desinformación como la creación, la presentación y la divulgación de información verificablemente falsa o engañosa con fines lucrativos o para engañar deliberadamente a la población, cuando esta pudiera causar un perjuicio público[22]. Dicho perjuicio público puede incluir el socavamiento de los procesos democráticos o las amenazas contra los bienes públicos como la salud, el medio ambiente y la seguridad.

A diferencia de los contenidos ilícitos (que abarcan el discurso de odio, los contenidos terroristas o los materiales de abuso sexual de menores), la desinformación atañe a contenido legal. Por lo tanto, interfiere en dos valores fundamentales y esenciales de la UE: la libertad de expresión y la libertad de prensa. De acuerdo con la definición de la Comisión, la desinformación no contiene la publicidad engañosa, los errores de información, la sátira ni la parodia o las noticias y los comentarios claramente identificados como partidistas.

14 Las nuevas tecnologías y programas informáticos permiten que la desinformación se propague fácilmente y de un modo relativamente barato a través de **las redes sociales y otros medios en línea**. La desinformación se concentra normalmente en temáticas sensibles tendentes a polarizar la opinión y agitar las emociones, por lo que es más probable que la gente la comparta. Entre dichas temáticas se incluyen aspectos sanitarios (por ejemplo, las campañas antivacunas), la inmigración, el cambio climático o cuestiones relacionadas con la justicia social.

Campañas de desinformación de terceros países para influir en los procesos democráticos

15 El objetivo de la desinformación consiste en polarizar el debate democrático, encender o avivar tensiones en la sociedad y socavar los sistemas electorales, y repercute ampliamente en las sociedades y la seguridad de Europa. En última instancia, menoscaba la libertad de opinión y expresión. La desinformación está a menudo **apoyada por agentes de terceros países** con el objetivo de desestabilizar nuestras sociedades y nuestros sistemas democráticos. En este contexto, las campañas

[22] Comisión Europea, *Comunicación sobre la lucha contra la desinformación en línea*, COM(2018) 236.

de desinformación a gran escala pueden implicar también el pirateo de redes. Sirva de ejemplo de lo anterior la campaña de influencia rusa en el referéndum del Reino Unido sobre la salida de la Unión Europea (véase el ***recuadro 6***).

Recuadro 6

Campañas rusas de desinformación contra los procesos decisorios democráticos[23]

A mediados de 2016, se puso en marcha una campaña por parte de agentes de Rusia para influir en la votación del referéndum del Reino Unido sobre su salida de la UE, celebrado en junio de 2016. Un análisis de los tuits concluyó que, en las 48 horas anteriores a la votación, más de 150 000 cuentas rusas tuitearon sobre el *#Brexit* y publicaron más de 45 000 mensajes al respecto. En el día del referéndum, las cuentas rusas tuitearon 1 102 veces con la etiqueta *#ReasonsToLeaveEU*.

16 Luchar contra la desinformación representa un gran reto, habida cuenta de la necesidad de encontrar el justo equilibrio entre la seguridad y nuestros derechos y libertades fundamentales, fomentando la innovación y un mercado abierto. La UE ha puesto en marcha una serie de medidas para **combatir la desinformación**.

- En 2015, se estableció el **Grupo de Trabajo East StratCom**, con sede en el SEAE, para contrarrestar las campañas rusas de desinformación[24]. Los expertos han alabado su trabajo para promocionar las políticas de la UE, apoyar a los medios de comunicación independientes de los países de la vecindad europea y prever, detectar y combatir la desinformación[25].

---

[23] Park advisors, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*, Christina Nemr y William Gangware, 2019.

[24] Conclusiones del Consejo Europeo EUCO 11/15, 20 de marzo de 2015. Desde entonces, se han añadido dos Grupos de Trabajo adicionales para los Balcanes Occidentales y la vecindad meridional de la UE.

[25] En un informe, el Consejo Atlántico instaba a la UE a pedir a todos los Estados miembros que enviaran expertos nacionales al Grupo de Trabajo. Véase: D. Fried y A. Polyakova, *Democratic Offense Against Disinformation*, 5 de marzo de 2018.

- En 2018, ENISA emitió una **comunicación sobre la lucha contra la desinformación en línea**[26]. Entre otras medidas cabe citar las destinadas a aumentar la fiabilidad de los contenidos y el apoyo a las iniciativas para una mayor formación mediática y sobre las noticias.

- El Centro Común de Investigación de la Comisión ha desarrollado un **código de buenas prácticas voluntario y autorregulado**, basado en instrumentos políticos existentes, al que se han adherido plataformas en línea y la industria publicitaria[27].

- También se ha creado una **red europea de verificadores de datos**.

La desinformación en tiempos de COVID-19 y la respuesta de la UE en la materia

17 La desinformación también ha sido un problema en el contexto de la **crisis sanitaria provocada por el COVID-19**[28] (véase el ***recuadro 7*** para consultar ejemplos de dicha desinformación).

[26] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation («Fake News")*, abril de 2018.

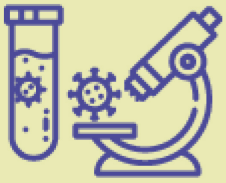
[27] JRC, *The digital transformation of news media and the rise of disinformation and fake news*, JRC Technical Reports, JRC Digital Economy Working Paper 2018-02, abril de 2018.

[28] Instituto Reuters y Universidad de Oxford, *Types, Sources, and Claims of Covid-19 Misinformation*, abril de 2020.

Recuadro 7

Ejemplos de desinformación relacionados con el COVID-19 comunicados por la Comisión[29]

Afirmaciones falsas, como «beber lejía o alcohol puro puede curar las infecciones causadas por el coronavirus», son todo lo contrario y pueden resultar muy peligrosas. **El centro toxicológico de Bélgica ha registrado un aumento del 15 % del número de accidentes relacionados con la lejía.**



Teorías conspiratorias, como la afirmación de que el coronavirus es una «infección causada por las élites mundiales para reducir el crecimiento de la población». Las evidencias científicas son claras: el virus forma parte de una familia de virus procedentes de animales entre los que se encuentran otros patógenos como los causantes del síndrome respiratorio agudo grave (SARS) y el síndrome respiratorio de Oriente Medio (MERS).

Afirmaciones no científicas según las cuales «las instalaciones de 5G están propagando el virus». Estas teorías, que no tienen justificación alguna, han provocado la destrucción de antenas.

18 En marzo de 2020, la Comisión, ENISA, CERT-UE y Europol emitieron una **declaración conjunta sobre las amenazas relacionadas con el COVID-19**[30], en la que indicaron que agentes malintencionados estaban aprovechando las complicadas circunstancias presentes durante esta crisis de salud pública para dirigirse a los teletrabajadores, las empresas y los particulares en general. Además, ENISA ha

[29] Comisión Europea, *Combatir la desinformación sobre el coronavirus*, sin fecha.

[30] Joint Statement European Commission, ENISA, CERT-EU and Europol, *Coronavirus outbreak*, 20 de marzo de 2020.

desplegado campañas informativas específicas para los sectores afectados por la desinformación durante la pandemia de COVID-19[31].

La verificación de los datos es decisiva para luchar contra la desinformación

19 La UE también ha redoblado sus esfuerzos por apoyar a los verificadores de datos y los investigadores sobre la desinformación europeos. En concreto, ha establecido un **Observatorio Europeo de los Medios de Comunicación Digitales** a fin de examinar y comprender mejor los fenómenos de la desinformación: los agentes implicados, los vectores, las herramientas, los métodos, las dinámicas de difusión, los objetivos preferentes y el impacto en la sociedad. Otros ejemplos de proyectos financiados por la UE que abordan la desinformación son PROVENANCE, SocialTruth, EUNOMIA y WeVerify.

20 En 2018, con su **Código de buenas prácticas en materia de desinformación**[32], la UE propuso el primer conjunto de normas de autorregulación a nivel mundial para luchar contra la desinformación. Este fue rubricado por plataformas, las principales redes sociales, anunciantes y la industria publicitaria en octubre de 2018. Entre los signatarios se cuentan Facebook, Twitter, Mozilla, Google y las asociaciones y los miembros de la industria publicitaria. Microsoft suscribió el Código de buenas prácticas en mayo de 2019. TikTok se adhirió al Código en junio de 2020.

Protección de las elecciones de 2019 al Parlamento Europeo

21 La legitimidad de nuestros sistemas democráticos europeos se basa en que un electorado informado exprese su voluntad democrática en el marco de unas **elecciones libres y justas**. Todo intento malicioso de socavar y manipular intencionadamente la opinión pública representa pues una grave amenaza para nuestras sociedades. El objetivo de las injerencias en las elecciones y en la infraestructura electoral puede ser influir en las preferencias de los votantes, en su participación o en el propio proceso electoral: en la votación real, el recuento de los votos y la comunicación de los resultados. Tras la celebración del referéndum del Reino Unido, las elecciones europeas de 2019 condujeron a las primeras acciones coordinadas entre los Estados miembros para **proteger la integridad de las elecciones**

[31] ENISA, *Fichas informativas relativas al COVID-19*, 2020.

[32] *EU Code of Practice on Disinformation*, septiembre de 2018.

democráticas: las elecciones al Parlamento Europeo, pero también las de ámbito nacional.

22 Como ya se ha indicado en lo que antecede, la Comisión emitió su **Comunicación sobre la lucha contra la desinformación en línea: un enfoque europeo**[33] en abril de 2018. En septiembre de 2018, esta encontró seguimiento en un **paquete electoral**[34] diseñado para proteger las elecciones de la UE y los Estados miembros de la desinformación y los ciberataques. El paquete se centraba en la protección de los datos, la transparencia de la propaganda y la financiación de los partidos políticos, la ciberseguridad y las elecciones, e incluía asimismo sanciones por el incumplimiento de las normas de protección de datos por parte de los partidos. Además, se llevó a cabo un **ejercicio conjunto** para poner a prueba la eficacia de las prácticas de respuesta y los planes de emergencia de la UE y los Estados miembros para proteger las elecciones al Parlamento Europeo (véase el ***recuadro 8***).

[33] Comisión Europea, *La lucha contra la desinformación en línea: un enfoque europeo*, COM(2018) 236 final.

[34] Comisión Europea, *Estado de la Unión de 2018*, septiembre de 2018.

Recuadro 8

ELEx19: protección de las elecciones de 2019 al Parlamento Europeo[35]

El ejercicio ELEx19 sobre la resiliencia de las próximas elecciones al Parlamento Europeo se puso como objetivo determinar maneras de prevenir, detectar y mitigar los incidentes de ciberseguridad que podrían afectar a las elecciones de 2019.

En función de diversos escenarios con amenazas e incidentes cibernéticos, el ejercicio permitió a los participantes:

hacerse una idea general del nivel de resiliencia (en términos de políticas adoptadas, capacidades disponibles y competencias) de los sistemas electorales de toda la UE;

impulsar la cooperación entre las autoridades pertinentes a escala nacional (incluidas las electorales y otros organismos y agencias relevantes);

poner a prueba los planes de gestión de crisis existentes, así como los procedimientos correspondientes para prevenir, detectar, gestionar y responder ante los ataques contra la ciberseguridad y las amenazas híbridas, como las campañas de desinformación;

mejorar la cooperación transfronteriza y fortalecer los vínculos con los grupos de cooperación pertinentes a escala de la UE (por ejemplo, la Red de Cooperación Electoral, el Grupo de Cooperación SRI y la Red de CSIRT);

determinar todas las demás posibles deficiencias, así como unas medidas de mitigación de riesgos adecuadas, que deben aplicarse antes de las elecciones al Parlamento Europeo.

Participaron en dicho ejercicio más de 80 representantes de los Estados miembros de la UE, junto con observadores del Parlamento Europeo, la Comisión y la Agencia de la Unión Europea para la Ciberseguridad.

---

[35] ENISA, *EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections*, 5 de abril de 2019.

23 Finalmente, en diciembre de 2018, el Consejo Europeo adoptó un **Plan de Acción contra la desinformación**[36] a fin de dar una respuesta coordinada y complementar los esfuerzos nacionales. Este plan entrañaba acciones específicas basadas en cuatro pilares: mejorar las capacidades de las instituciones de la Unión para detectar, analizar y sacar a la luz la desinformación, reforzar las respuestas coordinadas y conjuntas a la desinformación, movilizar al sector privado para luchar contra la desinformación, y sensibilizar y mejorar la resiliencia social.

Ciberseguridad en la UE: competencias, agentes, estrategias y legislación

La ciberseguridad es principalmente una responsabilidad de los Estados miembros

24 En la UE, la ciberseguridad atañe principalmente a la **responsabilidad de los Estados miembros**. Este es especialmente el caso en lo concerniente a la protección de información sensible sobre seguridad nacional. Todos los Estados miembros cuentan con una **Estrategia de Ciberseguridad Nacional** para ayudarlos a abordar los riesgos susceptibles de socavar la consecución de los beneficios económicos y sociales derivados del ciberespacio. Sin embargo, los Estados miembros siguen divergiendo en términos de su capacidad y su compromiso en materia de ciberseguridad.

25 La UE desempeña una función en la creación de un **marco normativo común** dentro del mercado único de la UE y la generación de las condiciones para que los Estados miembros trabajen juntos con eficacia en diferentes ámbitos políticos con relevancia para la ciberseguridad, como la justicia y los asuntos de interior, el mercado único, el transporte, la salud pública, la política de consumo y la investigación. En política exterior, la ciberseguridad afecta a la diplomacia y está cada vez más integrada en la emergente política de defensa y seguridad de la UE.

---

[36] Comisión Europea, Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, *Plan de Acción contra la desinformación*, JOIN(2018) 36 final. El plan consiste en: mejorar las capacidades de las instituciones de la UE para detectar, analizar y sacar a la luz la desinformación, reformar las respuestas coordinadas y conjuntas, movilizar al sector privado y sensibilizar y mejorar la resiliencia social.

26 Los principales **agentes** de la ciberseguridad **en la UE** se describen en el *recuadro 9* siguiente.

Recuadro 9

Principales agentes de ciberseguridad en la UE

El objetivo de la **Comisión Europea** es aumentar las capacidades y la cooperación en materia de ciberseguridad, reforzar el papel de la UE en el ámbito de la ciberseguridad e integrar este aspecto en otras políticas de la UE.

Numerosas agencias de la UE prestan apoyo a la Comisión, en particular **ENISA**, **EC3** y **CERT-UE**. La **Agencia de la Unión Europea para la Ciberseguridad** (conocida como **ENISA** en razón de su nombre original, *European Network and Information Security Agency*) es principalmente un organismo consultivo y respalda el desarrollo de políticas, la creación de capacidades y el aumento de la sensibilización. El **Centro Europeo de Ciberdelincuencia (EC3)** de Europol se creó para reforzar la respuesta policial de la UE ante la ciberdelincuencia. La Comisión cuenta con un **equipo de respuesta a emergencias informáticas (CERT-UE)**, que da apoyo a todas las instituciones, órganos y organismos de la UE.

El **Servicio Europeo de Acción Exterior (SEAE)** está al frente de la ciberdefensa, la ciberdiplomacia y la comunicación estratégica, y alberga centros de análisis e inteligencia. La **Agencia Europea de Defensa (AED)** tiene por objeto desarrollar capacidades de ciberdefensa.

En la UE, los Estados miembros actúan a través del **Consejo**, que cuenta con numerosos organismos de coordinación e intercambio de información (entre ellos, el Grupo Horizontal «Cuestiones Cibernéticas»). El **Parlamento Europeo** actúa como colegislador.

Las **organizaciones del sector privado**, tales como la industria, los organismos de gobernanza de internet y las instituciones académicas, son socios participantes en el desarrollo y la aplicación de las políticas, por ejemplo, a través de una asociación público-privada contractual (**APPc**).

La ciberestrategia de la UE: la ciberseguridad lleva siendo una importante preocupación desde 2013

27 La ciberseguridad lleva siendo una de las principales preocupaciones políticas al menos desde 2013, cuando la Comisión adoptó su **estrategia de ciberseguridad**[37]. La estrategia tiene cinco objetivos principales:

- aumentar la ciberresiliencia;
- reducir la ciberdelincuencia;
- desarrollar estrategias y capacidades de ciberdefensa;
- desarrollar recursos industriales y tecnológicos de ciberseguridad;
- establecer una política internacional del ciberespacio en consonancia con los valores fundamentales de la UE.

En años posteriores, otras estrategias de la UE abordaron también la cuestión de la ciberseguridad (véase el ***recuadro 10***).

[37] Comisión Europea, *Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro*, JOIN(2013) 1 final, 7 de febrero de 2013.

Recuadro 10

Otras estrategias de la UE que abordan la cuestión de la ciberseguridad

- La **Agenda Europea de Seguridad** (2015)[38], dirigida a mejorar la aplicación de la ley y la respuesta judicial ante la ciberdelincuencia, principalmente mediante la renovación y la actualización de la legislación y de las políticas existentes;
- La **Estrategia para el Mercado Único Digital** (2015)[39], encaminada a mejorar el acceso a bienes y servicios digitales: a tal efecto resulta esencial reforzar la seguridad en línea, la confianza y la inclusión;
- La **Estrategia Global de la UE** (2016)[40], que establece una serie de iniciativas para impulsar la función de la UE en el mundo. La ciberseguridad y la refutación de la desinformación mediante una comunicación estratégica formaron un pilar esencial al respecto.

28 Por añadidura, en 2017, la Comisión Europea y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad emitieron una **comunicación conjunta sobre la ciberseguridad de la UE**[41] al Parlamento Europeo y al Consejo, en la que abogaron por estructuras más robustas y eficaces para promover la ciberseguridad y responder a los ciberataques no solo en los Estados miembros, sino también en las instituciones, órganos y organismos de la Unión.

---

[38] Comisión Europea, *Agenda Europea de Seguridad*, COM (2015) 185 final, 28 de abril de 2015.

[39] Comisión Europea, *Una Estrategia para el Mercado Único Digital de Europa*, COM (2015) 192 final, 6 de mayo de 2015.

[40] SEAE, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, junio de 2016.

[41] Comisión Europea y Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, *Comunicación conjunta sobre resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE*, JOIN(2017) 450, 13 de septiembre de 2017.

29 En julio de 2020, la Comisión Europea actualizó su agenda de 2015 y adoptó la **Estrategia de la UE para una Unión de la Seguridad**[42] para 2020-2025, por la que se establece la ciberseguridad como una cuestión de importancia estratégica. En dicha estrategia, la Comisión destaca en especial el fenómeno conocido como amenazas híbridas, que implican tanto ciberataques como campañas de desinformación, con agentes estatales y no estatales de terceros países actuando conjuntamente con la intención de manipular el entorno informativo y atacar infraestructuras básicas.

La legislación de la UE en materia de ciberseguridad: la Directiva sobre seguridad de las redes y sistemas de información, el RGPD, el Reglamento sobre la Ciberseguridad y un nuevo mecanismo de sanciones

30 La pieza jurídica clave, pilar principal de la estrategia de ciberseguridad de 2013, es la **Directiva sobre seguridad de las redes y sistemas de información (Directiva SRI) de 2016**[43], el primer acto legislativo de la UE sobre ciberseguridad. El objeto de la Directiva es conseguir un nivel mínimo de capacidades armonizadas mediante la obligación impuesta a los Estados miembros de adoptar estrategias nacionales de SRI y crear puntos de contacto únicos y equipos de respuesta a incidentes de seguridad informática (CSIRT)[44]. Asimismo, establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales en sectores críticos y para los proveedores de servicios digitales.

31 Antes de mayo de 2018, los Estados miembros tenían que haber transpuesto **la Directiva SRI a su legislación nacional**. Asimismo, debían identificar los denominados «operadores de servicios esenciales» antes de noviembre de ese mismo año. La

---

[42] Comisión Europea, *Comunicación sobre la Estrategia de la UE para una Unión de la Seguridad*, COM (2020) 605 final, 24 de julio de 2020.

[43] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

[44] Estos están integrados en estructuras cooperativas establecidas por la Directiva, la red de CSIRT (compuesta por los CSIRT designados de los Estados miembros de la UE y el CERT-UE, y cuya secretaría es asumida por ENISA) y el Grupo de Cooperación (apoya y facilita la cooperación estratégica y el intercambio de información entre los Estados miembros, y la Comisión asume su secretaría).

Comisión Europea debe revisar periódicamente el funcionamiento de esta Directiva. De julio a octubre de 2020, como parte de su objetivo político clave consistente en construir una «Europa adaptada a la era digital», así como en consonancia con los objetivos de la Unión de la Seguridad, la Comisión celebró una consulta, cuyos resultados se utilizarían para una primera valoración y una evaluación de impacto *ex post* de la Directiva SRI.

32 Paralelamente, el **Reglamento General de Protección de Datos**[45] entró en vigor en 2016 y se aplica desde mayo de 2018. Su objetivo es proteger los datos personales de los ciudadanos europeos estableciendo normas sobre su tratamiento y difusión. Concede determinados derechos a los interesados e impone obligaciones a los responsables del tratamiento (proveedores de servicios digitales) en relación con el uso y la transferencia de información.

33 Además, el **Reglamento sobre la Ciberseguridad**[46] introduce por primera vez un marco de certificación de la ciberseguridad para todos los productos, servicios y procesos de la UE relacionados con las TIC. Esto conlleva que las empresas operativas en la UE se beneficiarán de tener que certificar sus productos, procesos y servicios relacionados con las TIC una sola vez y de que sus certificados gocen de validez en toda la UE. El Reglamento sobre la Ciberseguridad ha establecido asimismo la **Agencia de la Unión Europea para la Ciberseguridad** (ENISA, que sustituye a la anterior Agencia Europea de Seguridad de las Redes y de la Información). Le concede a dicha agencia el mandato de incrementar la cooperación operativa en el ámbito de la UE, ayudando a los Estados miembros que así lo soliciten a gestionar incidentes de ciberseguridad y apoyando la coordinación de la UE en el supuesto de crisis y ciberataques transfronterizos a gran escala.

34 Finalmente, en mayo de 2019, el Consejo estableció un instrumento jurídico que permite a la UE imponer **medidas restrictivas selectivas para responder a los**

---

[45] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

[46] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación, 17 de abril de 2019.

ciberataques que constituyan una amenaza externa para la UE o sus Estados miembros y disuadir de que estos se cometan[47]. En consecuencia, la UE dispone de capacidad jurídica para sancionar a aquellas personas físicas o jurídicas que:

- sean responsables de ciberataques o tentativas de ciberataques;
- ofrezcan apoyo financiero, técnico o material para esos ataques; o estén implicadas de otras formas.

En julio de 2020, el Consejo utilizó por primera vez estas nuevas prerrogativas (véase el ***recuadro 11***).

Recuadro 11

Mayor firmeza: la UE impone las primeras sanciones de su historia contra los ciberataques[48]

En julio de 2020, el Consejo impuso medidas restrictivas contra seis personas y tres entidades responsables de diversos ciberataques o implicadas en ellos. Se trata de una respuesta a, entre otros, el intento de ciberataque contra la Organización para la Prohibición de las Armas Químicas y los conocidos públicamente como «WannaCry», «NotPetya» y «Operation Cloud Hopper».

Entre las sanciones impuestas figuran la prohibición de viajar y la inmovilización de bienes. Además, las personas y entidades de la UE tienen prohibido poner fondos a disposición de aquellas que figuren en la lista.

---

[47] Decisión (PESC) 2019/797 del Consejo relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros, 17 de mayo de 2019.

[48] Decisión (PESC) 2020/1127 del Consejo, de 30 de julio de 2020, por la que se modifica la Decisión (PESC) 2019/797 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros.

Ciberseguridad y ciberdefensa

35 En los últimos años, el ciberespacio está cada vez más militarizado[49] y armado[50]. Se lo considera ya el quinto campo de batalla, además de los escenarios terrestre, marítimo, aéreo y espacial. En 2014 se adoptó un **marco político de ciberdefensa de la UE**, que fue actualizado en 2018[51]. La actualización de 2018 identifica prioridades, entre las que figura el desarrollo de capacidades en ciberdefensa, así como la protección de las redes de comunicación e información de la política común de seguridad y defensa de la UE (PCSD). La ciberdefensa también forma parte del marco de Cooperación Estructurada Permanente y de la cooperación UE-OTAN.

36 Los casos de utilización del ciberespacio con fines políticos y de poner a prueba y penetrar agresivamente en la ciberseguridad de la UE y los Estados miembros son ya comunes. Estas actividades de ciberespionaje y piratería informática —cuyos objetivos son los Gobiernos nacionales, las entidades políticas y las instituciones de la UE, con el fin de extraer y recabar información clasificada— sugieren que se están acometiendo sofisticadas operaciones de ciberespionaje y manipulación de datos contra la UE y sus Estados miembros. El **Marco común de lucha contra las amenazas híbridas** (2016) de la UE aborda las amenazas cibernéticas para las infraestructuras críticas y para los usuarios privados y subraya el hecho de que los ciberataques se pueden llevar a cabo también a través de campañas de desinformación en las redes sociales[52]. Señala

---

[49] Centro de Estudios Políticos Europeos, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, noviembre de 2018.

[50] El programa malicioso utilizado para el ataque de secuestro de Wannacry, que Estados Unidos, el Reino Unido y Australia atribuyeron a Corea del Norte, fue desarrollado y almacenado inicialmente por la Agencia de Seguridad Nacional de Estados Unidos para explotar vulnerabilidades de Windows.
Fuente: A. Greenberg, *WIRED*, 19 de diciembre de 2017. A raíz de los ataques, Microsoft condenó el almacenamiento de vulnerabilidades de *software* por los Gobiernos y reiteró su llamamiento en favor de un Convenio de Ginebra Digital.

[51] *Marco político de ciberdefensa de la UE (actualización de 2018)*, 14413/18, 19 de noviembre de 2018.

[52] Comisión Europea/Servicio Europeo de Acción Exterior, *Comunicación conjunta sobre la lucha contra las amenazas híbridas: Una respuesta de la Unión Europea*, JOIN(2016) 18 final, 6 de abril de 2016.

asimismo la necesidad de mejorar la sensibilización y la cooperación entre la UE y la OTAN, que se plasmó en las declaraciones conjuntas UE-OTAN de 2016 y 2018[53].

Gasto en ciberseguridad en la UE: disperso y rezagado

Menos gasto en ciberseguridad en la Europa de los Veintisiete que en EE. UU.

37 Resulta complicado estimar el gasto público en ciberseguridad, debido a su naturaleza transversal y a que a menudo no se puede distinguir del gasto informático general[54]. Dicho esto, los datos disponibles apuntarían a que el **gasto público en ciberseguridad** ha sido comparativamente bajo en la UE:

- En 2020, el presupuesto del Gobierno federal de EE. UU. destinado únicamente a cuestiones relacionadas con la ciberseguridad ascendió aproximadamente a **17 400 millones de dólares estadounidenses**[55].
- A modo de comparación, se calcula que la Comisión tiene un gasto público en ciberseguridad que oscila entre **1 000 y 2 000 millones de euros** al año para todos los Estados miembros de la UE (que, en conjunto, tienen aproximadamente el mismo PIB que EE. UU.)[56].

---

[53] Declaración conjunta del presidente del Consejo Europeo, el presidente de la Comisión Europea y el secretario general de la Organización del Tratado del Atlántico Norte, 8 de julio de 2016 y 10 de julio de 2018.

[54] Comisión Europea, COM(2018) 630 final, 12 de septiembre de 2018.

[55] La Casa Blanca, *Cybersecurity budget fiscal year 2020*.

[56] Comisión Europea, Documento de trabajo de los servicios de la Comisión: *Impact Assessment Accompanying the document «Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027»*, SWD(2018) 305 final, 6 de junio de 2018.

- El gasto público en ciberseguridad de muchos Estados miembros en porcentaje del PIB supone, según las estimaciones realizadas, **la décima parte de los niveles de EE. UU.**, o incluso menos[57].

2014-2020: la financiación de la UE para la ciberseguridad está dispersa en varios instrumentos diferentes

38 De conformidad con la Comisión[58], existen al menos **diez instrumentos diferentes** en virtud del presupuesto general de la UE a través de los cuales se pueden financiar las cuestiones en materia de ciberseguridad (véase el ***recuadro 12*** respecto de los principales programas en términos financieros). En total, la financiación de la UE para ciberseguridad no militar ascendió a **menos de 200 millones de euros al año** durante el período 2014-2020. Además, no hay ningún instrumento de financiación a escala de la UE que ayude a los Estados miembros a coordinar sus actividades de ciberseguridad.

[57] Centro de Estudios Estratégicos de La Haya, *Dutch investments in ICT and cybersecurity: putting it in perspective*, diciembre de 2016.

[58] Comisión Europea, *Impact assessment accompanying the proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres*, SWD(2018) 403 final, 12 de septiembre de 2018.

Recuadro 12

Programas de la UE de apoyo a proyectos de ciberseguridad (2014-2020)

- Los **programas de investigación Horizonte 2020** de la UE asignaron unos 600 millones de euros a proyectos de ciberseguridad y ciberdelincuencia para el período 2014-2020. Dicha suma comprende 450 millones de euros para la APPc («asociación público-privada contractual») en materia de ciberseguridad para 2017-2020, con la meta de atraer 1 800 millones de euros más del sector privado;

- los **Fondos Estructurales y de Inversión Europeos (EIE) prevén** una aportación de hasta 400 millones de euros para inversiones de los Estados miembros en ciberseguridad hasta el final de 2020;

- el **Mecanismo «Conectar Europa» (MCE)** financió inversiones por valor de unos 30 millones de euros al año. Estas comprenden la cofinanciación de los equipos de respuesta a emergencias informáticas (CERT) nacionales que los Estados miembros deben establecer en virtud de la Directiva SRI, por un importe aproximado de 13 millones de euros al año, de 2016 a 2018[59];

- el **Fondo de Seguridad Interior – Policía (FSI-Policía)** financia estudios, reuniones de expertos y actividades de comunicación; estas ascendieron a cerca de 62 millones de euros entre 2014 y 2017. Los Estados miembros también pueden recibir subvenciones para equipos, formación, investigación y recogida de datos en régimen de gestión compartida. Diecinueve Estados miembros han recibido estas subvenciones por un total de 42 millones de euros;

- el **Programa «Justicia»** proporcionó 9 millones de euros para apoyar la cooperación judicial y los tratados de asistencia jurídica mutua, especialmente el intercambio de datos electrónicos e información financiera.

[59] Artículo 9, apartado 2, de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (la «Directiva SRI»).

39 Además, se han asignado 500 millones de euros del presupuesto de la UE al **Programa Europeo de Desarrollo Industrial en materia de Defensa** en 2019 y 2020[60]. El programa se centra en mejorar la coordinación y la eficiencia del gasto en defensa de los Estados miembros a través de incentivos para el desarrollo conjunto. Su objetivo es generar a partir de 2020 un total de 13 000 millones de euros de inversión en capacidades de defensa, entre las que se cuenta la ciberdefensa, a través del Fondo Europeo de Defensa. Finalmente, en el marco de la **Iniciativa de Seguridad Europea**, el Banco Europeo de Inversiones aportará 6 000 millones de euros de financiación de doble uso (investigación y desarrollo/ciberseguridad y seguridad civil) entre 2018 y 2020[61].

2021-2027: el nuevo programa Europa Digital

40 Con sus conclusiones de julio de 2020 sobre el nuevo marco financiero plurianual (MFP) para el período 2021-2027, el Consejo decidió que el **programa Europa Digital**[62] invertiría en capacidades digitales estratégicas clave, como la informática de alto rendimiento, la inteligencia artificial y la ciberseguridad de la UE. Complementará otros instrumentos, en especial Horizonte Europa y el Mecanismo «Conectar Europa», para respaldar la transformación digital de Europa.

41 El Consejo ha decidido asignar 6 800 millones de euros al programa Europa Digital para el período 2021-2027, o sea, aproximadamente **970 millones de euros al año**. Se trata de un considerable aumento en comparación con el período de 2014-2020, pero sigue siendo menos que la propuesta inicial de la Comisión (8 200 millones de euros para el mismo período, dedicándose 2 000 millones de euros a fortalecer la industria de ciberseguridad de la UE y la protección social general, apoyando por ejemplo la implementación de la Directiva SRI).

---

[60] Comisión Europea, Reglamento (UE) 2018/1092 del Parlamento Europeo y del Consejo, de 18 de julio de 2018, por el que se establece el Programa Europeo de Desarrollo Industrial en materia de Defensa con el objetivo de apoyar la competitividad y la capacidad de innovación de la industria de la defensa de la Unión (DO L 200 de 7.8.2018, p. 30).

[61] Banco Europeo de Inversiones; *The EIB Group Operating Framework and Operational Plan 2018*, 12.12.2017.

[62] Comisión Europea, *Europe investing in digital: the Digital Europe Programme*, septiembre de 2020.

PARTE II – Descripción general de la labor de las EFS

Introducción

42 La ciberseguridad y nuestra autonomía digital se han convertido en cuestiones de importancia estratégica para la UE y sus Estados miembros. En los sectores público y privado de todos los Estados miembros existen numerosas deficiencias en la gobernanza de la ciberseguridad, aunque a diferentes niveles. Esto menoscaba nuestra capacidad para limitar los ciberataques y, llegado el caso, responder ante los mismos.

43 No obstante, en 2018, una encuesta de las Entidades Fiscalizadoras Superiores (EFS) en la UE demostró que alrededor de la mitad no había auditado nunca el ámbito de la ciberseguridad. Desde entonces, las EFS han dispuesto sus actividades de auditoría en materia de ciberseguridad, con un especial enfoque en la protección de los datos, la preparación de los sistemas contra los ciberataques y la protección de los sistemas de las empresas de servicios públicos esenciales. Analizaron asimismo otros aspectos muy pertinentes. Como es comprensible, no todas estas auditorías pueden hacerse públicas, puesto que pueden contener información sensible de seguridad nacional.

44 En razón de la importancia de la ciberseguridad para el funcionamiento de nuestras sociedades e instituciones políticas, el Comité de Contacto decidió dedicar el compendio de auditorías de este año a esta temática. En esta segunda parte se resumen los resultados de una selección de auditorías llevadas a cabo por las doce EFS de Estados miembros participantes y por el Tribunal de Cuentas Europeo en materia de ciberseguridad. Cada EFS participante aportó el informe sobre una de las auditorías seleccionadas, que se resume por añadidura en la tercera parte. Se acometieron muchas otras auditorías sobre esta cuestión, como reflejan los informes adicionales indicados por las EFS participantes.

Metodología de auditoría y temas cubiertos

45 En cuanto al tipo de auditoría llevada a cabo en los correspondientes informes de auditoría resumidos en el presente compendio, la mayoría de las EFS que contribuyeron habían realizado auditorías de gestión sobre temáticas relacionadas con la ciberseguridad, mientras que dos (las EFS de Polonia y Hungría) habían efectuado auditorías de conformidad y una (el Tribunal de Cuentas Europeo) había acometido una revisión de la política.

46 Al determinar su enfoque, la mayoría de las EFS establecieron que sus auditorías abarcaran al menos dos maneras de evaluar el objeto de las mismas: un examen de documentos estratégicos o políticas definidas (por ejemplo, nacionales) de alto nivel, un examen de procedimientos para evaluar su conformidad con la metodología COBIT establecida (véase el ***recuadro 13***) o un análisis de la eficacia de los sistemas de gestión informática instaurados. Una EFS (el Tribunal de Cuentas de los Países Bajos) llegó incluso a utilizar a piratas informáticos éticos para probar la eficacia de los sistemas de ciberseguridad en el control de las fronteras y las estructuras hídricas esenciales. En el ***recuadro 14*** resumimos esquemáticamente los métodos y las técnicas que emplearon las diversas EFS para llevar a cabo su labor de auditoría.

Recuadro 13

¿Qué son los COBIT?

Los objetivos de control para la información y tecnologías afines (COBIT, por sus siglas en inglés) constituyen un marco de mejores prácticas y procedimientos reconocidos para la gestión y la gobernanza de las tecnologías de la información definidos por la ISACA, la Asociación para la Auditoría y Control de Sistemas de Información. Ayudan a la organización a lograr objetivos estratégicos a través de un uso eficaz de los recursos disponibles y la minimización de los riesgos informáticos. Los COBIT interconectan la gobernanza de las empresas y de las tecnologías de la información. Esta vinculación se efectúa poniendo en relación las empresas con los objetivos informáticos, definiendo parámetros y modelos de madurez para ponderar la consecución de los objetivos y estableciendo las responsabilidades de los propietarios de las empresas y los procesos informáticos.

47 Las temáticas tratadas al auditar la ciberseguridad variaron en gran medida. Algunas EFS auditaron ámbitos de interés público muy concretos; la de los Países Bajos, por ejemplo, auditó la ciberseguridad de sus vitales sistemas de protección frente al mar y gestión del agua. Otras, como las EFS irlandesa y húngara, abordaron cuestiones más transversales, como la implementación de la estrategia de ciberseguridad nacional y la protección de los datos personales y los activos de datos nacionales. Sin embargo, todas las EFS trataron aspectos que podrían tener un impacto negativo en servicios o infraestructuras públicos.

48 Las EFS estonia y lituana reconocieron la importancia estratégica de los activos de datos nacionales, que revisten una importancia crucial en la seguridad nacional, y la protección de su integridad frente a los ciberataques externos. La EFS danesa consagró

una auditoría específicamente a evaluar la seguridad de cuatro organismos públicos frente a ataques con programas de secuestro. Las EFS neerlandesa, polaca y portuguesa auditaron la eficacia de diferentes sistemas informáticos de apoyo de los controles fronterizos (respectivamente, en el aeropuerto de Schiphol, la Comandancia Principal de Policía Fronteriza y el Ministerio de Asuntos Interiores y Administración en Polonia y las fronteras portuguesas), abordando así también la seguridad dentro de la UE.

Período de auditoría

49 Los informes de auditoría seleccionados contenidos en este compendio se publicaron entre 2004 y 2010. La mayoría tenía un período de auditoría que abarcaba dos años o más, aunque cuatro (los de Dinamarca, Estonia, Francia y Portugal) presentaban períodos de auditoría de un año.

Objetivos de auditoría

50 Las diversas EFS que han contribuido al presente compendio trataron un abanico de riesgos al llevar a cabo su labor de auditoría. Los riesgos abordados en sus aportaciones fueron: amenazas a los derechos individuales de los ciudadanos de la UE mediante el tratamiento inadecuado de los datos personales, riesgo de que las instituciones no puedan prestar un servicio público importante o de que lo hagan de manera limitada y graves consecuencias para la seguridad pública, el bienestar y la economía en el Estado miembro, así como para la ciberseguridad dentro de la UE. Al menos cuatro de las EFS (las de Estonia, Hungría, los Países Bajos y Portugal) englobaron tres o más de las temáticas mencionadas en sus informes de auditoría incluidos en el presente compendio.

51 La ciberseguridad sigue siendo una competencia de los Estados miembros. Sin embargo, como la legislación de la UE ha ganado en amplitud, pero también en especificidad con el paso del tiempo, la mayoría de las instituciones y organismos auditados por las EFS ya contribuye a la consecución de los objetivos estratégicos de la UE en materia de ciberseguridad, si bien no en la misma medida. Por ejemplo, la Oficina del interventor y auditor general de Irlanda auditó la implementación de la Directiva sobre Ciberseguridad de la UE, encaminada a aumentar la resiliencia de las redes y los sistemas de información clave, y prestó su asesoramiento sobre cómo

mejorarla. De manera similar, la auditoría de la Oficina Fiscalizadora Estatal de Hungría abordó el aspecto de la conformidad con las directivas de la UE existentes.

52 En el ***recuadro 14*** también se indica si el resultado de la auditoría contribuyó a un aumento de la ciberresiliencia de los auditados o a una reducción de la ciberdelincuencia, o si ayudaría a desarrollar políticas de ciberdefensa y fortalecer competencias, mejorar el desarrollo de tecnologías y lograr progresos en la cooperación a escala internacional, siendo estos en particular los principales objetivos de la estrategia de ciberseguridad de la UE. Las recomendaciones proporcionadas por las EFS abordaron en la mayoría de los casos más de dos de los objetivos estratégicos que la UE tiene previsto alcanzar.

53 Por añadidura, la labor de auditoría llevada a cabo por las EFS sirvió para detectar deficiencias de seguridad o implementación que indujeron a las instituciones auditadas a realizar esfuerzos adicionales. Por ejemplo, durante el trabajo de auditoría, cuatro instituciones analizadas en Dinamarca comenzaron ya a implementar varios de los controles de seguridad prospectivos a fin de incrementar significativamente el grado de protección frente a los ataques con programas de secuestro, a desarrollar capacidades de defensa y a incrementar la ciberresiliencia, reduciendo así su exposición a la ciberdelincuencia en el futuro.

54 Observamos asimismo que las recomendaciones de auditoría se presentaron en varios niveles de dirección y responsabilidad, dirigiéndose al Gobierno central, a ministerios y agencias de nivel operativo o a los propietarios de sistemas informáticos.

Recuadro 14

Descripción general de la labor de auditoría de las EFS respecto de las aportaciones realizadas al compendio (parte I)

Ámbito de interés principal		Dinamarca	Estonia	Irlanda	Francia	Letonia	Lituania	Hungría	Países Bajos	Polonia	Portugal	Finlandia	Suecia	UE (Tribunal de Cuentas Europeo)
Tipo de auditoría	De gestión	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	
	De conformidad							✓		✓				
	Análisis													✓
Enfoque de la auditoría	Examen de políticas	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓
	Examen de procedimientos	✓	✓		✓		✓	✓		✓	✓	✓		
	Examen de sistemas	✓			✓	✓	✓	✓	✓	✓	✓		✓	
	Evaluación de la solidez mediante pruebas directas								✓		✓			
Amenazas tratadas	Impacto en los derechos individuales		✓		✓			✓			✓			✓
	Impacto en infraestructuras o servicios públicos	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Impacto en la seguridad nacional		✓	✓		✓	✓	✓	✓		✓			
	Impacto en la seguridad dentro de la UE	✓							✓		✓			✓

Descripción general de la labor de auditoría de las EFS respecto de las aportaciones realizadas al compendio (parte II)

Ámbito de interés principal		Dinamarca	Estonia	Irlanda	Francia	Letonia	Lituania	Hungría	Países Bajos	Polonia	Portugal	Finlandia	Suecia	UE (Tribunal de Cuentas Europeo)
Objetivos estratégicos de la UE en materia de ciberseguridad abarcados	Aumentar la resiliencia cibernética	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
	Reducir la ciberdelincuencia	✓					✓							✓
	Desarrollar políticas y capacidades de defensa	✓	✓	✓		✓	✓	✓	✓	✓				✓
	Desarrollar recursos tecnológicos				✓	✓			✓				✓	
	Fomentar la cooperación internacional (políticas)			✓				✓						✓
Nivel del destinatario de las recomendaciones	Administración del Estado	✓	✓				✓					✓	✓	✓
	Operativo (ministerios y agencias)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Propietarios de sistemas informáticos	✓			✓			✓	✓	✓				

Principales observaciones de las auditorías

55 En las secciones siguientes se resumen las principales observaciones de auditoría realizadas por las EFS.

Auditorías de gestión

56 La ***Rigsrevisionen*** **danesa** evaluó si las instituciones gubernamentales esenciales seleccionadas gozaban de una protección satisfactoria frente a los programas de secuestro. Las instituciones gubernamentales son objetivos frecuentes de los ciberataques y los programas de secuestro son actualmente una de las mayores amenazas para la ciberseguridad. La auditoría concernió a la Autoridad Danesa de Datos Sanitarios, al Ministerio de Asuntos Exteriores, a Banedanmark (la red ferroviaria danesa) y a la Agencia Danesa de Gestión de Emergencias. Se seleccionaron estas cuatro instituciones porque son las responsables de prestar servicios esenciales en los campos de la salud, los asuntos exteriores, el transporte y la preparación ante emergencias, en los que garantizar el acceso a los datos puede tener una importancia vital. La auditoría reveló que ninguna de las cuatro contaba con una protección satisfactoria frente a los programas de secuestro. La labor de auditoría demostró que ninguna de las cuatro instituciones había implementado varios controles de seguridad comunes para mitigar los riesgos. La auditoría concluyó que era importante que las instituciones sopesaran la aplicación de controles de seguridad prospectivos con el fin de incrementar su resiliencia a los ataques con programas de secuestro.

57 La ***Riigikontroll*** **estonia** reconoció que la preservación de la independencia del país requiere no solo la defensa física del territorio, sino también la protección de los activos digitales con una importancia primordial para el Estado. Los activos digitales que necesitan más protección son los datos relativos a los ciudadanos, al territorio y la legislación. También requieren seguridad los datos relativos a los bienes muebles e inmuebles y los derechos de los residentes estonios. La Oficina de Auditoria estonia consideró la posibilidad de ciberamenazas en el supuesto de una escalada de problemas de seguridad. Dichos escenarios de riesgo y un incremento del número de incidentes de seguridad de la información, como los ciberataques y las filtraciones de datos, podrían poner en peligro los datos y las bases de datos de mayor importancia para el Estado. Por lo tanto, la auditoría analizó cómo determinó el Estado qué datos y bases de datos eran esenciales para garantizar la seguridad nacional. La auditoría concluyó que, a pesar de la implementación del sistema de seguridad de referencia

ISKE compuesto por tres niveles[63], que es obligatorio para las agencias estatales, había deficiencias significativas en lo referente a garantizar la seguridad de la información de varias bases de datos esenciales.

58 La ***Oficina del interventor y auditor general*** **irlandesa** revisó el progreso efectuado en materia de medidas de ciberseguridad desde el establecimiento del Centro de Ciberseguridad Nacional irlandés. El Centro, dirigido por el Departamento de Comunicaciones, Acción Climática y Medio Ambiente, se constituyó en 2011. Su principal misión es asegurar las redes gubernamentales, asistir a la industria y a los particulares a proteger sus propios sistemas y asegurar la infraestructura nacional esencial. La auditoría concluyó que, aunque el Centro de Ciberseguridad Nacional desempeñaba una función vital, el nivel de recursos asignados en sus primeros cuatro años de funcionamiento era notablemente inferior al previsto en un principio y la dirección estratégica general del Centro carecía de un plan estratégico. Por añadidura, se necesitaba más claridad en relación con las respectivas funciones de los organismos participantes en la investigación de los ciberdelitos y los incidentes de seguridad nacional. Por último, quedaban aún por implementar los requisitos de la Directiva sobre Ciberseguridad de la UE en relación con el desarrollo de una estrategia nacional.

59 La ***Cour des comptes*** francesa sometió a su escrutinio «*Parcoursup*», una nueva plataforma digital que funciona como una fuente de información sobre formaciones universitarias disponibles y condiciones de acceso, cuyo objetivo es fortalecer la concordancia entre la aptitud de los estudiantes de secundaria y sus resultados académicos con el contenido de los cursos de educación superior. La auditoría reveló que el Gobierno había centralizado correctamente el acceso a todos los estudios postsecundarios a través de la plataforma digital a fin de gestionar la expansión de la educación superior. No obstante, el sistema anterior se había adaptado apresuradamente para convertirse en el nuevo «*Parcoursup*», sin cambios estructurales importantes. Por tanto, no se subsanaron las vulnerabilidades del sistema de información en términos de seguridad, rendimiento y solidez. La plataforma sigue viéndose afectada por riesgos significativos en términos de la calidad y la continuidad del servicio público y la seguridad de los datos personales.

[63] ISKE es una norma de seguridad de la información desarrollada para el sector público estonio; es obligatoria para las organizaciones de la Administración estatal y local que gestionan bases de datos y registros.

60 La ***Valsts Kontrole*** **letona** completó una auditoría de gestión sobre la eficiencia de la infraestructura pública de tecnologías de la información y de las comunicaciones (TIC). El propósito de la auditoría era verificar si la Administración pública disponía de un enfoque unificado para la gestión eficaz de la infraestructura de TIC y si las instituciones habían evaluado las ventajas de la centralización. La auditoría reveló que las reticencias de las autoridades a gestionar la infraestructura de TIC de manera centralizada habían comportado el establecimiento de una serie de salas de servidores, lo que incrementaba significativamente los costes de mantenimiento. En la mayoría de dichas salas existían amenazas para la seguridad y los centros de datos no estaban suficientemente protegidos frente a accesos físicos y riesgos ambientales. Por añadidura, no se había introducido en las instituciones práctica alguna para llevar a cabo evaluaciones periódicas sobre si resultaría más barato mantener la infraestructura de TIC internamente, cooperar con otra institución o externalizar el mantenimiento de las TIC. La auditoría recomendó un sistema de supervisión periódico que permitiera evaluar toda la Administración pública como un único sistema.

61 La ***Valstybės kontrolė*** **lituana** reconoció la importancia de la implantación de recursos de información electrónica críticos del Estado, como la gestión de las finanzas gubernamentales, la Administración tributaria y la atención sanitaria. La pérdida de información esencial y la indisponibilidad de los correspondientes sistemas de información podrían tener graves consecuencias para la seguridad pública, el bienestar y la economía. La auditoría se centró en evaluar la gestión (control general) y la madurez de los recursos informativos críticos del Estado. Detectó problemas sistémicos tanto en la creación como en la ejecución de la política de recursos de información estatales y en su correspondiente mecanismo de gestión. La auditoría concluyó que un nivel bajo de madurez de los recursos informativos críticos del Estado apuntaba a debilidades en el diseño y la implementación de la correspondiente política, lo que redundaba en una mayor vulnerabilidad de los mismos. A fin de incrementar la seguridad de los recursos de información del Estado, se había de mejorar el mecanismo de gestión.

62 En 2018, el **Tribunal de Cuentas de los Países Bajos** decidió llevar a cabo auditorías sobre ciberseguridad en sectores esenciales para la sociedad. Los primeros dos sectores auditados fueron la gestión del agua y los controles fronterizos automatizados. El primero es vital para una nación en gran parte bajo el nivel del mar, y el segundo, debido a la posición del aeropuerto de Ámsterdam Schiphol como nodo internacional y puerta de entrada al país. El Ministro de Infraestructuras y Gestión del Agua ha designado una serie de infraestructuras hídricas gestionadas por la Dirección

General de Obras Públicas y Gestión del Agua (el auditado) como «componentes críticos» del sector de gestión del agua. Numerosos sistemas informáticos utilizados para manejar las estructuras hídricas esenciales se remontan a los años ochenta y noventa del siglo pasado, una época en la que por lo general no se tenía en cuenta la ciberseguridad. El Ministro de Defensa y el Ministro de Justicia y Seguridad comparten la responsabilidad de los controles fronterizos llevados a cabo por los guardias de fronteras en el aeropuerto de Schiphol. Ambos ministerios cuentan con sistemas informáticos utilizados por los guardias de fronteras. Los sistemas son esenciales para las operaciones aeroportuarias y se utilizan para el tratamiento de datos muy sensibles. Esto los convierte en un apetecible objetivo para los ciberataques dirigidos al sabotaje, al espionaje o a la manipulación de los controles fronterizos. La auditoría examinó si los auditados estaban preparados para afrontar las amenazas cibernéticas y si lo hacían eficazmente. En el caso de las estructuras hídricas, el auditado tenía aún trabajo por delante en términos tanto de detección como de respuesta a fin de cumplir sus propios objetivos de ciberseguridad. En cuanto a los controles fronterizos, se concluyó que las medidas de ciberseguridad no eran adecuadas ni tenían garantías de futuro.

63 El ***Tribunal de Contas* portugués** auditó los sistemas de información en los que se basan la concesión, la expedición y la utilización del pasaporte electrónico portugués (PEP), en especial en el control automático de pasajeros mediante la lectura de datos biométricos en las fronteras del país luso. La auditoría verificó el cumplimiento dela legislación nacional y de la UE y de las normas y directrices internacionales para la concesión, la expedición y la utilización del PEP, incluida la conformidad con el marco jurídico nacional. Examinó la eficacia de los procesos clave asociados al ciclo de vida del PEP, en especial los relacionados con su concesión, expedición y uso. La auditoría examinó asimismo aspectos críticos del rendimiento de los sistemas de información, en especial el cumplimiento de los requisitos de seguridad relativos a los sistemas de información del PEP (SIPEP).

64 La ***Valtiontalouden tarkastusvirasto* finlandesa** investigó si la ciberprotección en el Gobierno central era lo más eficaz y rentable posible. La auditoría se centró en cómo se gestionaba la ciberseguridad del Gobierno central. Entre las entidades auditadas se incluyeron las autoridades encargadas de regular la ciberprotección en el Gobierno central (la Oficina del Primer Ministro, el Ministerio de Hacienda y el Ministerio de Transporte y Comunicaciones), así como las autoridades responsables de las tareas de ciberprotección y servicios informáticos centralizados del Gobierno del Estado. En el Gobierno finlandés, la responsabilidad de la ciberprotección está descentralizada,

siendo cada organismo estatal responsable de su propia ciberseguridad. La auditoría recomendó que el Ministerio de Hacienda definiera e implementara un modelo completo de gestión operativa en caso de incidentes de ciberseguridad en los servicios de TIC del Gobierno central. Además, el Ministerio de Hacienda debería averiguar cómo abordar la ciberseguridad de los servicios, financiándolos a lo largo de su ciclo de vida, y mejorar el conocimiento sobre la situación operativa ordenando a las autoridades que comuniquen las ciberviolaciones al Centro de Ciberseguridad.

65 La ***Riksrevisionen*** **sueca** abordó la incidencia de sistemas informáticos obsoletos en la Administración del Estado para evaluar si el Gobierno y las autoridades habían tomado medidas adecuadas para evitar que los sistemas informáticos se convirtieran en un obstáculo para la digitalización efectiva. La auditoría detectó sistemas informáticos obsoletos en un gran número de agencias gubernamentales auditadas. En muchas de ellas, uno o varios sistemas informáticos esenciales para su actividad estaban obsoletos y una notable proporción de las agencias examinadas no mantenía un enfoque correcto con respecto al desarrollo y la administración de la asistencia informática. Gran parte de dichas agencias carecía de una descripción general de cómo estaban vinculados los procesos operativos, las estrategias y los sistemas. La conclusión general fue que la mayoría de las agencias no había logrado aún afrontar eficazmente los problemas dimanantes de unos sistemas informáticos obsoletos. La oficina de auditoría sueca considera que el problema es tan grave y está tan extendido que supone un obstáculo para continuar con una digitalización eficaz de la Administración estatal.

Auditorías de conformidad en materia de ciberseguridad

66 La ***Oficina Nacional de Auditoría*** **de Hungría** reconoció que la seguridad de los datos, como activos nacionales, constituye un interés fundamental de la sociedad para la preservación y la protección de los valores nacionales. Garantizar la mejora de la seguridad de los datos personales y públicos dentro de los activos de datos nacionales de Hungría resulta esencial para reforzar la confianza de los ciudadanos en el Estado y asegurar el funcionamiento correcto y continuo de la Administración pública. El propósito de la auditoría de conformidad sobre protección de datos era ponderar si se había establecido en Hungría un marco reglamentario y operativo para la protección de datos y si las principales organizaciones de gestión de datos habían cumplido los requisitos para la gestión segura de los datos y la externalización de su tratamiento. La auditoría concluyó que el reglamento interno de las organizaciones de gestión de datos sobre sus actividades de gestión de datos había garantizado la protección de los

activos de datos nacionales como parte de los activos nacionales, de conformidad con las disposiciones legales en vigor entre 2011 y 2015. Los responsables del tratamiento habían aplicado adecuadamente los requisitos y la transferencia de datos a terceros se había implementado correctamente.

67 La ***Najwyższa Izba Kontroli*** **polaca** evaluó la seguridad de los datos recogidos en los sistemas diseñados para prestar importantes servicios públicos. La auditoría abarcó seis instituciones seleccionadas, responsables de tareas públicas significativas. El grado de preparación e implementación del sistema de seguridad de la información no aportó un nivel de seguridad aceptable para los datos recogidos en los sistemas informáticos utilizados para prestar importantes servicios públicos. Los procesos de seguridad de la información se ejecutaban de forma desordenada e intuitiva ante la ausencia de procedimientos establecidos. De las seis unidades auditadas, solo una había implementado el sistema de seguridad de la información, aunque cabe señalar que su funcionamiento también contaba con defectos notables. La auditoría concluyó que se habían de desarrollar e implementar recomendaciones y requisitos generales relacionados con la seguridad informática a nivel central, para su aplicación a todas las entidades públicas.

Análisis sobre ciberseguridad

68 El ***Tribunal de Cuentas Europeo*** realizó un análisis panorámico de las políticas de ciberseguridad de la UE y detectó los retos principales para su aplicación eficaz. Abarcó la seguridad de las redes y de la información, la ciberdelincuencia, la ciberdefensa y la desinformación. En el análisis se detectaron varias deficiencias en la legislación de la Unión en materia de ciberseguridad y se señaló que los Estados miembros no habían transpuesto de manera coherente la legislación existente. Finalmente, en el análisis se llamó la atención sobre el hecho de que se carecía de datos fiables sobre los ciberincidentes en la UE y de que no había una visión completa sobre el gasto en ciberseguridad por parte de la UE y sus Estados miembros. En el análisis también se señalaron limitaciones de recursos que afectaban a las agencias pertinentes de la UE relacionadas con el ámbito cibernético, incluidas las dificultades de atraer y mantener el talento. Otro reto estaba relacionado con el desajuste entre la financiación de la ciberseguridad y los objetivos estratégicos de la UE.

PARTE III – Resumen de los informes de las EFS

Dinamarca
Rigsrevisionen

Protección frente a ataques con programas de secuestro

Fecha de publicación: 2017

Enlace al informe: Resumen del informe (versión en inglés)

Tipo y período de auditoría

Tipo de auditoría: Auditoría de gestión

Período auditado: De abril a septiembre de 2017

Resumen del informe

Tema de la auditoría

En este informe se analizó si las instituciones gubernamentales esenciales seleccionadas gozaban de una protección satisfactoria frente a los programas de secuestro.

Las instituciones gubernamentales son objetivos frecuentes de los ciberataques y los programas de secuestro son actualmente una de las mayores amenazas para la ciberseguridad. Los programas de secuestro son un *software* malicioso que bloquea el acceso a los datos. Generalmente, los programas de secuestro cifran los datos e impiden que las instituciones atacadas puedan utilizarlos. Los piratas informáticos exigen un rescate para descriptar los datos y permitir a las instituciones recobrar el acceso a los mismos. De lo anterior se desprende que los programas de secuestro representan una especial amenaza para la accesibilidad de los datos.

La incapacidad repentina de acceder a los datos puede dificultar a las instituciones la prestación de servicios importantes o incluso impedirles totalmente dicha prestación. Las instituciones afectadas por un ataque con un programa de secuestro se ven por lo general obligadas a desactivar una parte o la totalidad de su red informática para investigar el alcance de la agresión. Los ataques con programas de secuestro pueden

tener un impacto económico significativo, ya que las instituciones corren el peligro de sufrir una pérdida de la producción, por ejemplo, si se les impide acceder a su red informática o si pierden los datos recogidos y tratados durante un lapso prolongado de tiempo. En 2017, un ataque con un programa de secuestro contra el servicio sanitario nacional del Reino Unido conllevó la cancelación de 19 000 operaciones y citas. Por lo tanto, la dirección de las instituciones se debería centrar en el riesgo que suponen dichos ataques y en implementar los controles de seguridad necesarios para protegerse de los programas de secuestro y reducir el impacto de un posible ataque.

El estudio incluyó a la Autoridad Danesa de Datos Sanitarios, al Ministerio de Asuntos Exteriores, a Banedanmark (la red ferroviaria danesa) y a la Agencia Danesa de Gestión de Emergencias. Se seleccionaron estas cuatro instituciones porque son las responsables de prestar servicios esenciales en los campos de la salud, los asuntos exteriores, el transporte y la preparación ante emergencias donde el acceso a sus datos puede tener una importancia vital. La Autoridad de Datos Sanitarios presta asimismo servicios informáticos centralizados a la mayoría de organismos gubernamentales dependientes del Ministerio de Sanidad.

La finalidad del estudio era evaluar si las cuatro instituciones tenían una protección satisfactoria frente a los ataques con programas de secuestro efectuados a través del correo electrónico. Así, la *Rigsrevisionen* examinó veinte controles de seguridad comunes que ofrecen una protección básica frente a los programas de secuestro. Por añadidura, la EFS examinó cinco controles de seguridad que las instituciones deberían tener en cuenta en futuras evaluaciones de riesgos. Entre los controles prospectivos se cuentan, por ejemplo, las nuevas tecnologías que pueden reducir el número de correos electrónicos falsos recibidos por una institución o detectar y enviar alertas relativas a una actividad inusual en los ordenadores. El estudio fue iniciado por la *Rigsrevisionen* y se basó en las constataciones de cuatro auditorías informáticas llevadas a cabo de abril a septiembre de 2017. Dicho estudio refleja una imagen sobre el grado de protección de las instituciones frente a los programas de secuestro. Las instituciones tuvieron la oportunidad de implementar los veinte controles de seguridad comunes tras la conclusión de las auditorías informáticas. Por lo tanto, los resultados del estudio atañen solo a la protección de las instituciones frente a los programas de secuestro en el momento de las cuatro auditorías informáticas. El estudio ofrece una presentación del rendimiento de las cuatro instituciones, pero no incluye un análisis comparativo ni una clasificación de dicho rendimiento.

Constataciones y conclusiones

La *Rigsrevisionen* estimó que ninguna de las cuatro instituciones contaba con una protección satisfactoria frente a los programas de secuestro. El estudio muestra que las cuatro instituciones no habían implementado varios controles de seguridad comunes para mitigar los ataques. En particular, la Autoridad de Datos Sanitarios y Banedanmark presentaban notables deficiencias de ciberseguridad. Esto significaba que las cuatro instituciones estaban expuestas a un mayor riesgo de ataques con programas de secuestro por correo electrónico que les imposibilitarían prestar sus servicios durante diversos períodos de tiempo. Las cuatro instituciones han informado a la *Rigsrevisionen* de que desde la finalización del estudio han trabajado en la implementación de varios de los controles de seguridad para incrementar el grado de protección frente a los programas de secuestro.

La prevención contra los ataques con programas de secuestro instaurada por las instituciones, incluidas las amenazas tanto internas como externas, era inadecuada. Es especialmente preocupante que ninguna de las instituciones se asegurara de que los parches de seguridad estuvieran actualizados y que tres de ellas no hubieran aplicado una lista blanca para impedir la ejecución de programas maliciosos por parte del personal. Esto aumenta el riesgo de que los programas de secuestro infecten una parte o la totalidad de la red informática, así como su propagación.

En tres de las instituciones, la dirección no prestaba un nivel de atención suficiente a la amenaza que suponen los programas de secuestro y las evaluaciones de riesgo llevadas a cabo por la dirección de la Autoridad de Datos Sanitarios y Banedanmark no abarcaban todos los aspectos pertinentes. Esto significaba que las instituciones carecían de una evaluación actualizada de dicha amenaza y, por tanto, se encontraban en una posición débil para prevenir nuevos ataques y reducir el impacto de futuros incidentes. La dirección de la Autoridad de Datos Sanitarios y Banedanmark no estaba lo suficientemente concentrada en la evaluación de riesgos y, en consecuencia, la seguridad informática de estas dos instituciones no se basaba en prioridades definidas por sus responsables.

Tres de las instituciones no tenían instaurados unos planes de respuesta ante incidentes adecuados para ayudarlas a restablecer sus operaciones tras un ataque con un programa de secuestro. Resulta especialmente significativo que tres de las instituciones no comprobaran periódicamente si podrían restablecer los datos y los sistemas afectados por un ataque con un programa de secuestro. Tal extremo incrementa el riesgo de pérdida de los datos albergados por dichas instituciones en el

ámbito del ataque con un programa de secuestro y de que las mismas no puedan prestar sus servicios durante un período de tiempo prolongado.

Los escenarios de riesgo están cambiando constantemente y por ello es importante que las instituciones consideren la implementación de controles de seguridad prospectivos para aumentar su resiliencia a los ataques con programas de secuestro, o sea, controles que faciliten la verificación de la identidad de los remitentes de los correos electrónicos y puedan detectar y filtrar los correos electrónicos potencialmente perjudiciales. Las cuatro instituciones están trabajando actualmente en algunos de dichos controles prospectivos de seguridad, que pueden contribuir a mejorar su protección frente a los ataques con programas de secuestro.

Otros informes en este ámbito

Título del informe:	Informe sobre la protección de datos de investigación en las universidades danesas
Enlace al informe:	Resumen del informe (versión en inglés)
Fecha de publicación:	2019

Título del informe:	Informe sobre la protección de los sistemas informáticos y los datos sanitarios en tres regiones de Dinamarca
Enlace al informe:	Resumen del informe (versión en inglés)
Fecha de publicación:	2017

Título del informe:	Informe sobre la gestión de la seguridad informática de los sistemas contratada a proveedores externos
Enlace al informe:	Resumen del informe (versión en inglés)
Fecha de publicación:	2016

Título del informe:	Informe sobre el acceso a los sistemas informáticos que apoyan la prestación de servicios esenciales para la sociedad danesa
Enlace al informe:	Resumen del informe (versión en inglés)
Fecha de publicación:	2015

Estonia
Riigikontroll

Garantía de la seguridad y preservación de bases de datos estatales esenciales en Estonia

Fecha de publicación: Mayo de 2018

Enlace al informe: Resumen del informe (versión en inglés)
Informe (versión en estonio)

Tipo y período de auditoría

Tipo de auditoría: Auditoría de gestión

Período auditado: 2017

Resumen del informe

Tema de la auditoría

La preservación de la independencia estonia requiere no solo la defensa física de su territorio, sino también la protección de los activos digitales con una importancia primordial para el Estado en relación con los eventos que planteen una mayor amenaza. Los activos digitales que necesitan más protección son los datos relativos a los ciudadanos, al territorio y la legislación. También requieren seguridad los datos relativos a los bienes muebles e inmuebles y los derechos de los residentes estonios.

La Oficina Nacional de Auditoría analizó cómo determinó el Estado qué datos y bases de datos eran esenciales para garantizar la seguridad nacional. Se comprobó la protección de la seguridad y la continuidad de dichos datos y bases de datos, incluida una descripción general de las herramientas utilizadas para la protección.

Habida cuenta de que Estonia es ahora miembro de la OTAN y de la Unión Europea, su seguridad física está mejor garantizada que antes de dicha adhesión. Sin embargo, Estonia ha de considerar la posibilidad de ciberamenazas en el supuesto de una escalada de problemas de seguridad. Dichos escenarios de riesgo y un incremento del número de incidentes de seguridad de la información, como los ciberataques y las

filtraciones de datos, podrían también poner en peligro los datos y las bases de datos de mayor importancia para el Estado. Si dichos datos de importancia primordial para el Estado se llegaran a modificar sin autorización, filtrar o perder, el Estado no podría llevar a cabo funciones necesarias como garantizar la seguridad de los ciudadanos, prestar servicios básicos, crear un clima empresarial adecuado, etc. Estonia tiene previsto gastar en un principio aproximadamente un millón de euros en almacenar datos esenciales en el extranjero.

Preguntas de auditoría

- ¿Determinaron los ministerios todas las bases de datos y requisitos de manipulación esenciales?
- ¿Están protegidos los registros y las bases de datos esenciales?
- ¿Está garantizada la continuidad a largo plazo de los datos y las bases de datos esenciales?

Constataciones

La Oficina Nacional de Auditoría realizó las observaciones siguientes sobre las bases de datos esenciales auditadas:

- No se habían establecido planes de acción o requisitos para la implementación del concepto de bases de datos esenciales. No se habían determinado las condiciones para seleccionar las bases de datos esenciales y no se contaba con la certeza de que estuvieran incluidas en el proceso todas las bases de datos necesarias. La protección adicional de las bases de datos se había organizado de manera informal y no suponía una obligación para sus propietarios, motivo por el cual los datos de cinco bases de datos esenciales no tenían una copia de seguridad en el extranjero.
- En las bases de datos esenciales no se habían establecido normas de seguridad de la información adicionales. Por otro lado, ni el sistema de seguridad de la información ISKE (una norma de seguridad de la información desarrollada para el sector público estonio y obligatoria para las organizaciones gubernamentales estatales y locales que gestionan bases de datos y registros), ni ningún acto jurídico o norma incluían requisitos adicionales para las bases de datos esenciales, como el almacenamiento de copias de seguridad de los datos fuera de Estonia. Se habían realizado copias de seguridad de las bases de datos auditadas, pero no se

había ensayado la recuperación del funcionamiento de los sistemas de información a partir de ellas.

- La implementación de ISKE y las auditorías correspondientes supusieron un problema con respecto a las bases de datos esenciales. En el momento de la auditoría, no se habían realizado auditorías de ISKE en dos de las diez bases de datos; tan solo se organizaron al final de esta auditoría (30 de noviembre de 2017). Solo se habían auditado dos bases de datos esenciales con la frecuencia impuesta por la legislación. También hubo casos en los que los problemas destacados por el auditor no se habían subsanado durante el tiempo transcurrido entre dos auditorías de ISKE (dos o tres años).

- Durante la auditoría, la Oficina Nacional de Auditoría descubrió que en algunas bases de datos esenciales no se habían implementado importantes medidas de seguridad de la información. Por ejemplo, en las directrices de seguridad de la información no se habían determinado los requisitos para una evaluación periódica de las vulnerabilidades de los sistemas de información, no se habían llevado a cabo controles o análisis periódicos de los registros de incidencias, no había planes de formación sobre la seguridad de la información o análisis de la sensibilización al respecto en el ámbito gubernamental sobre el que se basan dichos planes de formación, en algunos casos no se había inspeccionado la integridad de los archivos y no se habían llevado a cabo pruebas externas de penetración.

Conclusiones y recomendaciones

En la auditoría se constató que a pesar de la implementación del sistema de seguridad de referencia de tres niveles ISKE, cuyo uso es obligatorio para las agencias estatales y sus auditorías, había deficiencias significativas en lo referente a garantizar la seguridad de la información de varias bases de datos esenciales, como el análisis de los registros, las pruebas de penetración y la protección de los dispositivos móviles. No se habían establecido aún los requisitos especiales necesarios para proteger los datos esenciales.

El Ministerio de Economía y Comunicaciones había lanzado las primeras actividades necesarias para la protección de los datos esenciales, pero el proyecto de bases de datos esenciales estaba en una fase en la que requeriría un conjunto de normas jurídicamente vinculantes. Tampoco se contaba con un análisis de riesgos detallado o un plan de acción para el futuro.

Las copias de seguridad de cinco bases de datos esenciales estaban almacenadas en embajadas ubicadas en países extranjeros, pero en la hipótesis de la destrucción física de los centros de datos ubicados en Estonia, no estaría garantizada la preservación de los datos esenciales en las cinco bases de datos restantes.

Se hicieron dos recomendaciones generales:

- Determinar normas para la protección adicional de bases de datos esenciales, incluida su selección, el tratamiento de los datos que contienen y la copia de seguridad de los datos más importantes para el Estado, y evaluar cómo proporcionar una financiación adicional para estas actividades.

- Analizar las diferentes fases del establecimiento de bases de datos tanto en términos de planificación financiera como de seguridad de la información e instaurar las mejores prácticas de gestión de proyectos en la implementación de dichas etapas.

Oifig an Ard-Reachtaire Cuntas agus Ciste
Office of the Comptroller and Auditor General

Irlanda
Oficina del interventor y auditor general

Medidas relacionadas con la ciberseguridad nacional

Fecha de publicación: Septiembre de 2018

Enlace al informe: Resumen del informe (versión en inglés)

Tipo y período de auditoría

Tipo de auditoría: Auditoría de gestión

Período auditado: 2011-2018

Resumen del informe

Tema de la auditoría

El Departamento de Comunicaciones, Acción Climática y Medio Ambiente es el responsable de la política de ciberseguridad en Irlanda. El Departamento se responsabiliza asimismo, a través del Centro de Ciberseguridad Nacional, de coordinar la respuesta de emergencia gubernamental ante cualquier incidente de ciberseguridad a escala nacional.

El Centro de Ciberseguridad Nacional se constituyó en 2011. Su principal misión es asegurar las redes gubernamentales, asistir a la industria y a los particulares a proteger sus propios sistemas y asegurar la infraestructura nacional esencial.

Preguntas de auditoría

Este examen revisa el progreso efectuado en materia de medidas de ciberseguridad desde el establecimiento del Centro de Ciberseguridad Nacional. En concreto, analiza las cuestiones relacionadas con:

- la misión y los recursos del Centro;

- la Estrategia de Ciberseguridad Nacional (2015-2017);
- la implementación de la Directiva sobre Ciberseguridad de la UE;
- las disposiciones de gobernanza y vigilancia.

Constataciones y conclusiones

Aunque con la decisión gubernamental sobre el establecimiento del Centro de Ciberseguridad Nacional se aprobó una financiación anual de 800 000 euros, los fondos anuales recibidos efectivamente para la ciberseguridad entre 2012 y 2015 ascendieron a menos de un tercio de dicho importe. En 2017, la asignación se incrementó hasta 1,95 millones de euros. El personal del Centro casi se duplicó durante 2017, hasta los 14,5 equivalentes en tiempo completo. En 2018 se aprobó la designación de dieciséis efectivos más.

La Estrategia de Ciberseguridad Nacional (2015-2017) estableció doce medidas que se habían de lograr durante su vida útil. Con fecha de mayo de 2018, se habían completado cuatro medidas, cuatro se habían implementado parcialmente y otras cuatro no se habían aplicado aún.

El objetivo de la Directiva sobre Ciberseguridad de la UE es mejorar la resiliencia de las redes y los sistemas de información clave. En una evaluación del progreso logrado por Irlanda respecto de cada uno de los tres pilares de la Directiva se constató lo siguiente:

- *Pilar 1: mejorar las capacidades de ciberseguridad de los Estados miembros de la UE.* Implementado parcialmente: se han abordado requisitos estructurales, pero siguen existiendo deficiencias en la planificación estratégica.
- *Pilar 2: facilitar la cooperación entre los Estados miembros de la UE en materia de ciberseguridad.* Implementado.
- *Pilar 3: introducir medidas de seguridad y obligaciones en cuanto a la comunicación de incidentes en los sectores clave.* Implementado parcialmente: queda trabajo por hacer en relación con la identificación de las redes y los sistemas de información esenciales, la designación formal de entidades como los operadores de servicios esenciales y la gestión de los proveedores de servicios digitales.

La decisión gubernamental (de julio de 2011) por la que se aprobó el establecimiento del Centro de Ciberseguridad Nacional también conllevaba el establecimiento de un

comité interdepartamental para instaurar y aplicar políticas a fin de abordar los desafíos de ciberseguridad en Irlanda. Aunque el grupo se reunió en cinco ocasiones entre 2013 y 2015, solo estaban disponibles para su revisión las actas de una de dichas reuniones. El comité lleva desde 2015 sin reunirse.

El Plan de Implementación de la Estrategia de Ciberseguridad Nacional establece la publicación de un informe anual y la realización de una evaluación de impacto formal de su labor para el final de 2017. Dichas actividades siguen pendientes, aunque el trabajo del Centro se expone en el informe anual del Departamento,

desde el que se solicitó formalmente una evaluación del rendimiento del Centro. No se aportaron pruebas de que se haya efectuado dicha evaluación. El Departamento indicó que la evaluación de rendimiento de la labor del Centro de Ciberseguridad Nacional formaba parte de su gestión del rendimiento y gobernanza corporativa ordinarias.

La auditoría concluye lo siguiente:

- Aunque el Centro de Ciberseguridad Nacional desempeña una función vital, el nivel de recursos asignados en sus primeros cuatro años de funcionamiento era notablemente inferior al previsto en un principio.
- La dirección estratégica general del Centro no está clara y no hay actualmente instaurado ningún plan estratégico.
- Se requiere más claridad en relación con las respectivas funciones de los organismos participantes en la investigación de los ciberdelitos y los incidentes de seguridad nacional.
- Quedan por implementar los requisitos de la Directiva sobre Ciberseguridad de la UE en relación con el desarrollo de una estrategia nacional.
- Aunque se han recomendado estructuras de gobernanza, no está claro cómo funcionan en la práctica sus mecanismos de gobernanza.

Existe una falta de transparencia con respecto a la disponibilidad y el coste de los recursos dedicados a la ciberseguridad.

Francia
Cour des comptes

Acceso a la educación superior: una evaluación inicial de la ley relativa a la orientación y al éxito de los estudiantes

Fecha de publicación: Febrero de 2020

Enlace al informe: Informe (versión en francés)

Tipo y período de auditoría

Tipo de auditoría: Auditoría de gestión

Período auditado: 2019-2020

Resumen del informe

Tema de la auditoría

El objetivo de la Ley relativa a la orientación y al éxito de los estudiantes (*loi relative à l'orientation et à la réussite des étudiants*, ORE), de 2018, era mejorar las tres fases principales en la trayectoria seguida por los jóvenes al acceder a la educación superior: orientación y apoyo para los estudiantes de bachillerato, selección de asignaturas y éxito en los primeros años de estudios. La Ley introdujo «*Parcoursup*», una nueva plataforma digital que funciona como un recurso de información sobre asignaturas disponibles y condiciones de acceso, cuyo objetivo es fortalecer la concordancia entre la aptitud de los estudiantes de secundaria y sus resultados con el contenido de las asignaturas de educación superior.

Los primeros dos años de la ORE fueron testigos del primer paso hacia la transformación del acceso a la educación superior. A pesar de numerosas dificultades, el despliegue de «*Parcoursup*» se había realizado de forma satisfactoria, si bien seguía careciendo de garantías de seguridad y sostenibilidad y los datos se podían haber aprovechado mejor, habida cuenta de su importancia.

La ORE se promulgó para resolver dos grandes problemas de la política educativa. El primero era el elevado índice de abandono entre los estudiantes universitarios. El segundo era que la antigua plataforma digital había acarreado una profunda insatisfacción porque empleaba una selección aleatoria en su fase final.

La reforma de la ORE recibió financiación por valor de 867 millones de euros a lo largo de cinco años. Se basaba en la noción de una continuidad entre los 3 últimos años de secundaria y los 3 primeros años universitarios, con el principio subyacente de que cuanto más sepan los estudiantes de bachillerato sobre el contenido de las asignaturas de educación superior, mayores serán las probabilidades de éxito en los exámenes, puesto que elegirán las formaciones que más se ajusten a sus aptitudes y ambiciones. La ORE buscaba poner fin a las deficiencias en la orientación disponible para los estudiantes del último tramo de secundaria y, así, reducir el cambio de formaciones, cuyo coste la *Cour* estimaba que ascendía a casi 550 millones de euros al año tan solo respecto del primer año de educación superior.

Los auditores llevaron a cabo una evaluación inicial del acceso a la educación superior en el contexto de la ORE, analizando los problemas de seguridad informática planteados por la plataforma.

El sistema de información se caracterizaba por una expansión de los factores de carga (la inclusión en 2020 de todas las formaciones de educación superior y un rápido aumento del número de usuarios en tan solo unos años). Esto reflejó el cambio precipitado de la anterior plataforma a «*Parcoursup*» sin cambiar de arquitectura, lo que generó unos riesgos significativos en términos de la calidad, la continuidad, la adaptabilidad y el desarrollo adicional del servicio. Los puntos débiles del sistema en los ámbitos de la seguridad, del rendimiento y de la solidez no se habían corregido. «*Parcoursup*» se pudo configurar rápidamente porque fue gestionada en modo beta por un grupo acotado de profesionales muy capacitados y motivados, pero este enfoque conllevó que el sistema careciera de dirección estratégica y de una gobernanza satisfactoria.

Los auditores evaluaron la calidad del sistema de información y el rendimiento de la nueva plataforma «*Parcoursup*». «*Parcoursup*» se estableció en virtud de la ORE con el objetivo de mejorar la calidad de la orientación hacia formaciones de educación superior y, así, aumentar el porcentaje de graduados.

Constataciones

Aunque «*Parcoursup*» funcionaba satisfactoriamente, la plataforma estaba expuesta a riesgos informáticos, que se habían de mitigar. Se requerían garantías sobre su seguridad y sostenibilidad y, además, los datos se podrían haber aprovechado en mayor medida.

Un sistema de información antiguo

No había muchas novedades en «*Parcoursup*», ya que heredó la rigidez y la fragilidad de la anterior plataforma «*Admission Post-Bac*» (APB), junto con numerosos riesgos sin resolver. El sistema de información que constituye la base estructural de «*Parcoursup*» se adoptó directamente de la plataforma anterior. A pesar de promocionarse como una nueva herramienta de orientación, el corazón del sistema de información solo se había modificado ligeramente desde la APB. De hecho, más del 72 % de la infraestructura de información estaba intacta y solo se había reescrito algo menos del 30 % del código de la APB.

La base tecnológica de la plataforma se diseñó a principios de la década de los 2000 para gestionar alrededor de un millón de solicitudes para unas 100 000 plazas cada año, pero el alcance del sistema de información se amplió para gestionar un flujo anual de en torno a 10 millones de solicitudes para aproximadamente un millón de plazas. «*Parcoursup*» surgió como una herramienta antigua con una nueva imagen. El aumento de la carga planteó dudas sobre la capacidad de la plataforma para lograr su fin previsto.

Un sistema de información con una documentación deficiente

A pesar de los esfuerzos de transparencia del Ministerio, el 99 % del código fuente de «*Parcoursup*» seguía siendo cerrado. Lo poco que se había publicado revestía un interés limitado para comprender, valorar y evaluar el proceso de asignación de los solicitantes a los cursos.

Al igual que su predecesor, «*Parcoursup*» era un sistema de información operativo con una documentación deficiente. Los resultados de la auditoría del código sugirieron que la aplicación era de baja calidad y alto riesgo y la auditoría detectó numerosas violaciones críticas. El sistema era de peor calidad que otros programas con una antigüedad similar y tenía un elevado riesgo de fallos.

«*Parcoursup*» utilizaba código fuente tanto abierto como cerrado. El código abierto presentaba una tasa mucho más alta de violaciones críticas que el cerrado, lo que significaba que las perturbaciones en el servicio suponían un riesgo. La plataforma

tampoco estaba a salvo de los piratas informáticos (auditoría de seguridad del código fuente de julio de 2018). Sin embargo, al final de 2019 el Ministerio anunció que había comenzado un procedimiento de certificación para el código de «*Parcoursup*».

La documentación existente del código fuente no era ni coherente ni exhaustiva. El código de «*Parcoursup*» era anormalmente complejo. Los auditores consideraron que el código fuente debía reestructurarse para reducir el número de componentes complejos.

La arquitectura del sistema de información «*Parcoursup*» era de alto riesgo: de hecho, la base de datos aún se gestionaba de una manera arcaica, o sea, manualmente. La fragilidad del sistema respondía a su intensa dependencia de la disponibilidad y la vigilancia del operador. El Ministro reconoció que la arquitectura de «*Parcoursup*» comportaba grandes riesgos y que estos no se podrían corregir sin un desarrollo adicional de la aplicación.

El sistema de información «*Parcoursup*» presentaba una documentación deficiente y se basaba fundamentalmente en los conocimientos técnicos del personal de la agencia gubernamental nacional (*Service à Compétence Nationale,* SCN). A modo de documentación había comentarios escritos en la base de datos que se encontraba en el corazón del sistema, lo que hacía difícil mantener y desarrollar el sistema de información y explotar los datos. La información de los usuarios almacenada en la plataforma no se podía extraer y evaluar fácilmente sin una investigación en profundidad. Habida cuenta de la ausencia de documentación técnica estructurada, la capacidad del SCN para desempeñar sus tareas estratégicas dependía totalmente del responsable del centro informático.

Estrategia de seguridad: son necesarias mejoras

Debido a la sensibilidad de los datos personales contenidos en el sistema, «*Parcoursup*» presenta todo un desafío de seguridad. En principio, todas las organizaciones que gestionan un sistema de información deben contar con una política formal escrita de seguridad de los sistemas de información. A pesar de que el Primer Ministro lo reconoció como un proveedor de servicios esenciales, «*Parcoursup*» carecía de dicha política y era necesario tomar medidas inmediatas para instaurar una.

Cada equipo de «*Parcoursup*» tenía un responsable de seguridad de los sistemas de información adscrito al centro informático. Una buena práctica hubiera sido adscribir estos responsables directamente al Director del SCN, a fin de garantizar su independencia.

A mediados de 2019, seguían en curso las operaciones para alinear «*Parcoursup*» con el RGPD. Había determinadas medidas todavía pendientes, en especial la necesidad de establecer formalmente los diversos procedimientos utilizados para el tratamiento. La seguridad de los datos personales seguía siendo inadecuada y todavía se almacenaban demasiados datos individuales exhaustivos.

La unidad de «*Parcoursup*» estaba bajo la supervisión tanto del director del proyecto «*Parcoursup*», asignado por el gabinete del Ministro, como del departamento de estrategia formativa y asuntos estudiantiles de la Dirección General de Enseñanza Superior e Inserción Profesional, lo que generaba un conflicto de apoyos. Las cuestiones prácticas relacionadas con el sistema de información «*Parcoursup*» se abordaban en reuniones semanales. Aunque esta forma de organización tenía la ventaja de unos plazos de reacción rápidos en lo referente a la gestión cotidiana de los flujos de estudiantes, dejaba a «*Parcoursup*» sin un mando estratégico.

Por último, el sistema no era lo suficientemente transparente. No permitía aprovechar al máximo los datos almacenados en la plataforma, a pesar de su enorme potencial, cuya movilización redundaría muy probablemente en un mejor rendimiento.

Conclusiones y recomendaciones

El Gobierno había centralizado correctamente el acceso a los estudios postsecundarios a través de una plataforma digital que combinaba todos los programas formativos a fin de gestionar la generalización de la educación superior. El sistema anterior se había adaptado apresuradamente como «*Parcoursup*», pero sin cambios estructurales de peso. Por lo tanto, no se habían subsanado las vulnerabilidades del sistema de información en términos de seguridad, rendimiento y solidez, a pesar de que el incremento de la carga estaba destinado a persistir, habida cuenta del objetivo último de incluir todas las formaciones del tercer ciclo de estudios. Además, el sistema tenía una documentación deficiente, con un enfoque poco profesional con respecto al desarrollo informático, y su inusual complejidad aumentaba los riesgos de error en el supuesto de cualesquiera cambios operativos. La plataforma se encontraba, por tanto, rodeada de riesgos significativos en términos de la calidad y la continuidad del servicio público y la seguridad de los datos personales.

La *Cour des comptes* hizo las recomendaciones siguientes:

- el equipo de tecnologías de la información del SCN debe contar con más personal y se debía reorientar la financiación de la ORE para mejorar los recursos humanos y financieros de la Subdirección de sistemas de información e investigación estadística;
- el sistema de información se debe establecer a largo plazo mediante la corrección de sus defectos más urgentes, la modernización o reforma de su arquitectura y la documentación de las principales bases de datos tanto del antiguo sistema como de «*Parcoursup*» de una manera sistemática y estructurada;
- se debe dotar al sistema de información «*Parcoursup*» de una política de seguridad;
- se debe establecer un órgano de dirección conjunto para que el Ministerio de Educación y Juventud y el Ministerio de Enseñanza Superior, Investigación e Innovación supervisen la plataforma «*Parcoursup*», redirigiendo los recursos de la financiación de la ORE para actividades de «orientación».

Letonia
Valsts Kontrole

¿Ha aprovechado la Administración pública todas las oportunidades para una gestión eficaz de la infraestructura de TIC?

Fecha de publicación: Junio de 2019

Enlace al informe: Resumen del informe (versión en inglés)

Tipo y período de auditoría

Tipo de auditoría: Auditoría de gestión

Período auditado: 2017-2019

Resumen del informe:

Tema de la auditoría

La Oficina Nacional de Auditoría de Letonia completó una auditoría de gestión sobre la eficiencia de la infraestructura pública de TIC. El propósito de la auditoría era verificar si la Administración pública tenía un enfoque unificado con respecto a la gestión eficaz de la infraestructura de TIC y si las instituciones habían evaluado los beneficios de la centralización. Por añadidura, se determinó que la seguridad de los centros de datos era un factor importante al evaluar las opciones para una planificación adicional de la optimización.

Las reticencias de las autoridades a gestionar la infraestructura de TIC de manera centralizada, al menos en el ámbito de un ministerio, habían comportado el establecimiento de una serie de salas de servidores, lo que incrementó significativamente los costes de mantenimiento. En los cuatro ministerios auditados, se descubrió que sus 22 entidades subordinadas utilizaban 38 centros de datos. Durante la auditoría, la Oficina Nacional de Auditoría presenció situaciones en las que sistemas de información de importancia significativa, incluso nacional, estaban ubicados en instalaciones con un nivel de seguridad insuficiente. Optimizar el número

de salas de servidores no solo posibilitaría reducir los gastos de TIC, sino que también podría ofrecer un nivel de seguridad suficiente con un coste menor. Por otra parte, las instituciones ya contaban con salas de servidores de alta seguridad, pero no se estaban utilizando en toda su capacidad.

Principal objeto de la auditoría

El objetivo de la auditoría era verificar la creación y la implementación de todas las condiciones previas para la gestión unificada de la infraestructura de TIC, a fin de promover un uso más eficiente y seguro de los recursos de las TIC.

Constataciones y conclusiones

Gobernanza y optimización de las TIC

- Tanto a escala nacional como en los ministerios se carecía de una perspectiva a largo plazo del desarrollo y la optimización de las TIC. Los ministerios y sus entidades subordinadas optimizaron la infraestructura de TIC de conformidad con sus propias ideas y capacidades.

Entre 2011 y 2017, los costes totales de mantenimiento de las TIC de las instituciones auditadas aumentaron de 17 a 20 millones de euros al año. No se introdujo en las instituciones práctica alguna para llevar a cabo evaluaciones periódicas sobre si resultaría más barato mantener la infraestructura de TIC internamente, cooperar con otra institución o externalizar el mantenimiento de las TIC. Ni la centralización ni la descentralización de las TIC se consideran un objetivo *per se*, sino que hace falta un análisis de la situación y las alternativas específicas para aportar claridad sobre los costes existentes y las posibles alternativas.

Seguridad de las TIC

- El marco jurídico no definía claramente los requisitos de seguridad de la infraestructura de TIC en un sistema lógico en función de la importancia de la información tratada. No había requisitos técnicos detallados para la protección de los centros de datos de TIC.

- Las deficiencias en requisitos de seguridad conllevaban una costosa protección o, por el contrario, la protección de la información de importancia nacional no estaba garantizada. Había incluso sistemas de información importantes alojados en centros de datos de baja seguridad.

- En la mayoría de salas de servidores existían amenazas para la seguridad: los centros de datos no estaban suficientemente protegidos frente a accesos físicos y riesgos ambientales. En aras de la prevención de las amenazas para la seguridad, se necesitaban al menos entre 247 000 y 765 000 euros, en función del enfoque elegido, para, entre otras cuestiones: 1) mejorar las salas de servidores que contengan los sistemas de información más importantes y garantizar el almacenamiento de los recursos de TIC significativos en centros de datos de alta seguridad; o 2) mejorar todas las salas de servidores existentes. Sin embargo, esto exigiría inversiones por un importe que los auditores no podían justificar a menos que se minimizara el número de centros de datos.

El marco jurídico estaba incompleto, ya que se carecía de unos requisitos de seguridad detallados para la infraestructura de TIC. Por ejemplo, había requisitos para diversos criterios relativos a la seguridad lógica, pero no para la protección física y medioambiental de la infraestructura, que también afecta a la disponibilidad de los sistemas y la protección de los datos. Aunque en los documentos de planificación de las políticas públicas se destacaba la importancia de la seguridad de la infraestructura de TIC y la necesidad de fortalecerla, nadie había previsto actividades específicas en este ámbito. La falta de una diferenciación, clara, rastreable y lógica de los requisitos de seguridad planteaba el riesgo de que los requisitos de seguridad para tratar una información de igual importancia y relevancia pudieran variar dentro del país.

La seguridad en el espacio digital era objeto de una supervisión central por parte del Estado y era este quien respondía ante los incidentes, pero la responsabilidad de la implementación de la seguridad de la infraestructura informática se dejaba en manos de los responsables de las instituciones. Así, la perspectiva de cada una de ellas en cuanto a las cuestiones de seguridad de las TIC, la evaluación de la importancia de la información tratada y los recursos a disposición de las instituciones para abordar cuestiones de seguridad de las TIC variaban enormemente.

Se requería un sistema de supervisión periódica de estos procesos, a fin de evaluar toda la Administración pública como un único sistema, de manera independiente y utilizando unos criterios normalizados, a efectos de determinar los diferentes planteamientos y prevenirlos mediante la identificación de riesgos comunes, así como para planificar medidas preventivas encaminadas a mitigarlos.

Lituania
Valstybės Kontrolė

Gestión de los recursos informativos críticos del Estado

Fecha de publicación: Junio de 2018

Enlace al informe: Resumen del informe (versión en inglés)
Informe (versión en lituano)

Tipo y período de auditoría

Tipo de auditoría: Auditoría de gestión

Período auditado: 2014-2017

Resumen del informe

Tema de la auditoría

Mediante el uso de recursos informativos críticos del Estado —información electrónica crítica—, se desarrollan importantes funciones gubernamentales, como gestión de las finanzas públicas, la administración tributaria y la atención sanitaria. Cualquier pérdida de información esencial o la indisponibilidad de los correspondientes sistemas de información podrían tener graves consecuencias para la seguridad pública, el bienestar y la economía. Las evaluaciones del control informático general llevado a cabo por la Oficina Nacional de Auditoría de Lituania de 2006 a 2016 revelaron problemas recurrentes en la gestión de las TI (planificación, definición de la arquitectura de la información, estructura organizativa, cambios, garantía de la continuidad de la actividad, seguridad de los datos y supervisión y evaluación de la gestión informática). La Oficina llevó a cabo una auditoría de los recursos informativos críticos del Estado a fin de evaluar su gestión y seguridad y prever medidas de mejora.

La auditoría tenía como objetivo evaluar la gestión (control general) y la madurez de los recursos informativos críticos del Estado y detectar problemas sistémicos.

La Oficina valoró la madurez de la gestión informática en 12 organizaciones del sector público[64] que gestionan 44 sistemas de información estatales de primera categoría. La auditoría se llevó a cabo con arreglo a los requisitos de auditoría pública y las Normas Internacionales de las Entidades Fiscalizadoras Superiores. La evaluación se efectuó de conformidad con la metodología COBIT[65] en los siguientes ámbitos de mayor riesgo: planificación estratégica de las TI, determinación de la arquitectura informativa, gestión del riesgo informático, gestión de los cambios, garantía de una prestación ininterrumpida del servicio, seguridad del sistema, gestión de los datos, supervisión y evaluación de las actividades informáticas y garantía de la gestión informática. La valoración del proceso comprendía la gestión de las TI tanto a escala organizativa como nacional y la interacción entre dichos niveles de gestión.

Constataciones de la auditoría

Las tendencias en los cambios en el grado de madurez en relación con la gestión de los recursos informativos críticos del Estado eran positivas. Sin embargo, habida cuenta del creciente nivel de amenazas cibernéticas, los progresos observados eran demasiado lentos y se debía incrementar la seguridad de dichos recursos debido a las siguientes insuficiencias:

- El sistema para determinar los recursos informativos críticos del Estado no era lo suficientemente eficaz para permitir la instauración de soluciones de seguridad que satisfagan las necesidades reales:
  - Las evaluaciones diseñadas para demostrar la importancia esencial de los recursos de información del Estado carecían de objetividad, los cambios no siempre se evaluaban en las reevaluaciones, el proceso no contaba con una

[64] Inspección Tributaria del Estado, Centro Empresarial Estatal de Registros, Departamento de Tecnologías de la Información y de las Comunicaciones, Consejo del Fondo Nacional de la Seguridad Social, Centro Nacional de Información Agrícola a Empresas y Economía Rural, Centro del Sistema de Información Aduanera, Servicio Nacional de Alimentación y Veterinaria, Oficina del Parlamento de la República de Lituania, Ministerio de Hacienda, Comité de Desarrollo de la Sociedad de la Información, Seguro Nacional de Enfermedad y Servicio Forestal Nacional.

[65] Los COBIT (objetivos de control para la información y tecnologías afines) son un estándar de la organización internacional ISACA que establece las mejores prácticas para la gestión informática.

supervisión a escala nacional y las directrices para determinar la criticidad no garantizaban una implementación efectiva.

— El sistema para la identificación de los recursos informativos críticos del Estado y la infraestructura de información esencial no estaba normalizado; los recursos y la infraestructura se determinaban de diferentes maneras en función de la importancia de la información y los servicios, lo que complicaba el proceso de identificación de dichos recursos.

— No se había desarrollado ninguna arquitectura de información nacional para representar los sistemas de información estatales y sus interrelaciones, demostrar la escala de los recursos informativos críticos del Estado y posibilitar la toma de decisiones informadas sobre la importancia de los mismos.

- La gestión de los recursos informativos del Estado debía estar más en consonancia con las mejores prácticas y las normas de gestión informática a fin de lograr una mejora integrada del ámbito de las TI que contribuyera a lograr mejores progresos en la gestión de los recursos informativos críticos del Estado:

  — La planificación de las TI no era sostenible: las herramientas informáticas previstas se presentaban en diferentes documentos y se carecía de todo enfoque sistemático debido al exceso de documentos estratégicos, lo que dificultaba la determinación de las prioridades clave y la canalización de recursos para gestionar las mayores amenazas.

  — La supervisión de las TI no garantizaba que las organizaciones midieran la eficiencia de las operaciones informáticas y que las auditorías llevadas a cabo por los gestores de los recursos informativos críticos del Estado demostraran la madurez real de la gestión informática. La gestión informática estatal no era objeto de escrutinio a escala nacional y los problemas de gestión informática no se analizaban sistemáticamente. Se había creado un sistema para supervisar el cumplimiento por parte de los recursos de información estatales de los requisitos de seguridad de la información electrónica, destinado únicamente a facilitar la vigilancia del cumplimiento en materia de seguridad, pero no se aprovechaban lo suficiente sus funciones.

- Las medidas para garantizar la resiliencia de los recursos de información críticos al nivel de ciberamenazas no eran lo suficientemente eficaces; por tanto, seguía existiendo un riesgo de vulnerabilidad de dichos recursos:

— Era necesario aumentar la eficacia de la evaluación de los riesgos de seguridad informática, ya que no se detectaban todos los riesgos pertinentes y su metodología de evaluación no cumplía las prácticas de gestión informática más recientes; la gestión oportuna de los riesgos inaceptables no estaba garantizada.

— No se empleaban sistemáticamente medidas de seguridad organizativa susceptibles de reducir las amenazas cibernéticas. Las pruebas de la seguridad insuficientes, la formación incompleta del personal durante el desarrollo, la actualización y la modificación de los sistemas de información; las configuraciones y actualizaciones seguras de los programas informáticos no gestionadas; la gestión inadecuada de la continuidad de la actividad informática y los archivos de copias de seguridad ponían en entredicho la recuperación de las operaciones en curso; las mediciones del rendimiento en materia de seguridad eran insuficientes y no contribuían a la mejora de la seguridad.

Conclusiones

De media, la gestión informática de las entidades del sector público auditadas a lo largo de los diez últimos años logró el primer nivel de madurez de cinco[66] y había alcanzado un nivel de 1,7 en el momento de redactarse este documento. Este escaso nivel de madurez de los recursos informativos críticos del Estado apuntaba a insuficiencias en la formulación y la implementación de la política de recursos informativos del Estado, lo que redundaba en una mayor vulnerabilidad de los mismos. A fin de incrementar la seguridad de tales recursos, es necesario mejorar el mecanismo de gestión de los recursos de información del Estado para que se conforme al máximo a las mejores prácticas. Los auditores reseñaron asimismo que las medidas para garantizar la resistencia de los recursos de información críticos ante las amenazas cibernéticas no eran lo suficientemente eficaces. En consecuencia, la evaluación de los riesgos de seguridad informática ha de ganar en eficiencia, prestando una mayor atención a las pruebas de seguridad al crear y modernizar los sistemas de información y el personal docente.

[66] Con arreglo a la metodología COBIT.

Otros informes en este ámbito

Título del informe:	¿Se está combatiendo eficazmente la ciberdelincuencia?
Enlace al informe:	Resumen del informe (versión en inglés) Informe (versión en lituano)
Fecha de publicación:	2020

Título del informe:	Entorno de ciberseguridad en Lituania
Enlace al informe:	Resumen del informe (versión en inglés) Informe (versión en lituano)
Fecha de publicación:	2015

Hungría
Oficina Nacional de Auditoría

Auditoría sobre protección de datos: auditoría del marco nacional de protección de datos y determinados registros de datos prioritarios en el marco de la cooperación internacional

Fecha de publicación: Marzo de 2017

Enlace al informe: Informe (versión en húngaro)

Tipo y período de auditoría

Tipo de auditoría: De conformidad

Período auditado: 2011-2015

Resumen del informe

Tema de la auditoría

La seguridad de los activos de datos nacionales es del interés fundamental de la sociedad en cualquier país para la preservación y la protección de los valores nacionales. En consecuencia, garantizar la mejora de la seguridad de los datos personales y públicos en los activos de datos nacionales de Hungría resulta esencial para reforzar la confianza de los ciudadanos en el Estado y asegurar el funcionamiento correcto y continuo de la Administración pública. Por ende, la protección de los datos y la red de seguridad que proporciona el marco jurídico para su aplicación tienen una importancia fundamental para la sociedad.

En relación con el ámbito de la protección de datos, la Administración pública desempeña una función primordial en la gestión de los registros más voluminosos y sensibles de datos pertenecientes a activos de datos nacionales. Los responsables del tratamiento de los registros trabajan en estrecha cooperación a fin de cumplir sus cometidos. Transfieren periódicamente registros con grandes volúmenes de datos y deben prestar atención a los requisitos legales destinados a su protección. El uso de sistemas de información electrónicos para gestionar y tratar los datos es esencial hoy

en día, por lo que su funcionamiento adecuado y fiable ha de garantizarse mediante unos controles adecuadamente diseñados y gestionados.

Durante sus auditorías, la Oficina Nacional de Auditoría de Hungría hace gran hincapié en la protección de datos. Dicha Oficina acometió exhaustivas auditorías de protección de datos de 2011 a 2015 y publicó su informe en el primer trimestre de 2017. La auditoría abarcó asimismo aspectos de auditorías internacionales llevadas a cabo en paralelo en cooperación con el Grupo de Trabajo de Tecnologías de la Información de EUROSAI, que atañían principalmente a la conformidad con las directivas de la Unión Europea existentes.

El propósito de la auditoría de conformidad sobre protección de datos en Hungría era valorar si se había establecido en Hungría un marco reglamentario y operativo para la protección de datos y si las principales organizaciones de gestión de datos habían cumplido los requisitos para la gestión segura de los datos y la externalización de su tratamiento. En particular, la auditoría se centró en la protección de los datos personales y los activos de datos nacionales.

En el contexto de la auditoría, la Oficina evaluó la gestión de datos de seis organizaciones de gestión de datos (por ejemplo: autoridad tributaria, Hacienda nacional, seguro de enfermedad, pago de pensiones, oficina de educación, datos personales y registros sobre direcciones, vehículos y desplazamientos, y agencias administrativas para la gestión de datos penales), así como las actividades de la autoridad de protección de datos y la autoridad de seguridad de la información.

La auditoría prestó una atención especial al mandato de las organizaciones de gestión de datos, en particular en el caso de la transferencia de datos a terceros. Durante la auditoría de los controles internos sobre gestión y tratamiento de datos, se evaluó la existencia de normas actualizadas sobre las obligaciones, las responsabilidades y las competencias, así como la gestión y los procesos de recursos humanos.

Respecto a los sistemas electrónicos empleados en la gestión de los datos, la Oficina valoró las correspondientes medidas de seguridad, incluidos los ámbitos de la protección física, los derechos de acceso, el registro, los procedimientos de evaluación de la seguridad, la seguridad del sistema y las comunicaciones y el cumplimiento de la clasificación de la seguridad de la organización en su conjunto.

La externalización del tratamiento de datos se auditó con arreglo a los contratos estipulados, observando si las organizaciones de gestión de los datos obligaban a las entidades de tratamiento a cumplir los requisitos en materia de actividades de tratamiento de datos de acuerdo con las disposiciones legislativas.

Constataciones y conclusiones

A partir de la auditoría, la Oficina Nacional de Auditoría de Hungría constató que el reglamento interno de las organizaciones de gestión de datos sobre sus actividades garantizaba la protección de los activos de datos nacionales como parte de los activos nacionales, de conformidad con las disposiciones legales en vigor entre 2011 y 2015. En la práctica, los responsables del tratamiento habían aplicado correctamente los requisitos de seguridad en la gestión de los datos y la externalización de su tratamiento. La transferencia de datos a terceros se implementó con el mandato oportuno y una nítida distinción de responsabilidades y poderes.

Con respecto a determinados responsables del tratamiento, se concluyó que la clasificación de seguridad de los sistemas electrónicos y la organización en su conjunto no estaba siempre en consonancia con los requisitos legales, pero la amplitud de las deficiencias no afectaba sustancialmente a la seguridad de los datos tratados. Con arreglo a las recomendaciones incluidas en el informe de auditoría, las organizaciones de gestión de datos subsanaron dichas carencias en el marco de planes de acción aprobados por la Oficina.

En relación con la auditoría internacional paralela llevada a cabo en cooperación con el Grupo de Trabajo de Tecnologías de la Información de EUROSAI, la Oficina constató que la legislación de protección de datos húngara estaba en consonancia con la directiva de la UE existente.

En conclusión, al auditar la protección de datos, la Oficina Nacional de Auditoría de Hungría contribuyó a la correcta gobernanza y a la protección de los activos de datos nacionales.

Otros informes en este ámbito

Título del informe:	Informe – Auditorías de seguimiento – Auditoría de protección de datos – Auditoría del marco nacional de protección de datos y determinados registros de datos clave en el marco de la cooperación internacional
Enlace al informe:	Informe (versión en húngaro)
Fecha de publicación:	2020

Países Bajos
Tribunal de Cuentas

Ciberseguridad de las estructuras de gestión del agua esenciales y los controles fronterizos en los Países Bajos

Fechas de publicación: Marzo de 2019 y abril de 2020

Enlace a los informes: Resumen del informe sobre ciberseguridad y estructuras hídricas esenciales (versión en inglés)

Resumen del informe sobre ciberseguridad y controles fronterizos automatizados (versión en inglés)

Tipo y período de auditoría

Tipo de auditoría: Auditoría de gestión

Período auditado: 2018-2020

Resumen del informe

Tema de la auditoría

En 2018, el Tribunal de Cuentas de los Países Bajos decidió llevar a cabo auditorías de ciberseguridad en sectores esenciales para la sociedad. Con arreglo a su dilatada experiencia en auditar el cumplimiento de la seguridad de la información en el Gobierno central, el Tribunal de Cuentas consideró el valor añadido de auditar el *rendimiento* de las políticas y las medidas en la práctica. Los primeros dos sectores auditados fueron la gestión del agua y los controles transfronterizos automatizados; el primero es vital para una nación en gran parte bajo el nivel del mar y el segundo, por la posición que ocupa el aeropuerto de Ámsterdam Schiphol como nodo internacional y puerta de entrada al país.

El Ministro de Infraestructuras y Gestión del Agua ha designado una serie de infraestructuras hídricas gestionadas por la Dirección General de Obras Públicas y Gestión del Agua (el auditado) como «componentes críticos» del sector de gestión del agua. Numerosos sistemas informáticos utilizados para manejar las estructuras

hídricas esenciales se remontan a los años ochenta y noventa del siglo pasado, una época en la que por lo general no se tenía en cuenta la «ciberseguridad». Estos sistemas se diseñaron en un principio para su funcionamiento autónomo, pero se han ido conectando paulatinamente con redes informáticas mayores, por ejemplo, a fin de facilitar su operatividad a distancia. Esta tendencia ha hecho que los sistemas sean más vulnerables a las amenazas cibernéticas.

El Ministro de Defensa y el Ministro de Justicia y Seguridad comparten la responsabilidad de los controles fronterizos llevados a cabo por los guardias de fronteras en el aeropuerto de Schiphol. Ambos ministerios (los auditados) cuentan con sistemas informáticos que son empleados por los guardias de fronteras. Los sistemas son esenciales para las operaciones aeroportuarias y se utilizan para el tratamiento de datos muy sensibles. Esto los convierte en un apetecible objetivo para los ciberataques dirigidos al sabotaje, al espionaje o a la manipulación de los controles fronterizos.

Las auditorías examinaron la manera en que los auditados estaban preparados para afrontar las amenazas cibernéticas y si lo hacían eficazmente.

- Preguntas de auditoría con el objetivo de responder a las siguientes preguntas: ¿Cómo *protegen* los auditados los sistemas de las amenazas cibernéticas y *previenen* los ciberataques?
- ¿Cómo *detectan* los auditados las amenazas cibernéticas y los ciberataques?
- ¿Cómo *responden* los auditados en una situación de ciberataque?

En ambas auditorías, la atención se centró especialmente en la eficacia. En estrecha cooperación con los auditados, piratas informáticos éticos trabajaron en las estructuras hídricas esenciales y uno de los sistemas de control fronterizo. Huelga decir que se dio respuesta a todas las constataciones de las pruebas antes de la publicación de los informes y que no se revelaron detalles técnicos.

La principal diferencia entre las dos auditorías era que la relativa a las estructuras hídricas se centró en la consecución de los objetivos del auditado, mientras que la referida a los controles fronterizos se basó en el marco de ciberseguridad del NIST.

Constataciones

En primer lugar, ambas auditorías concluyeron que los auditados eran conscientes de las amenazas cibernéticas y estaban adoptando ya un enfoque profesional sobre el asunto.

No obstante, en el caso de las estructuras hídricas, el auditado tenía aún trabajo por delante en términos tanto de detección como de respuesta a fin de cumplir sus propios objetivos de ciberseguridad. El auditado estableció un Centro de Operaciones de Seguridad para detectar y responder a los ciberataques Sin embargo, el objetivo fijado para el final de 2017, consistente en detectar al instante cualesquiera ciberataques dirigidos contra estructuras hídricas esenciales, no se había logrado aún en otoño de 2018. Esto significaba que existía el riesgo de no detectar un ciberataque dirigido contra una estructura hídrica esencial o de descubrirlo demasiado tarde. Por añadidura, la prueba realizada en una de dichas estructuras reveló que era posible acceder físicamente a ella. Los piratas informáticos consiguieron entrar en la sala de control, donde se encontraron solos frente a puestos de trabajo sin asegurar. Por último, el auditado no había elaborado ningún escenario que contemplara una crisis causada por un ciberataque, y la información relativa a la respuesta se había omitido o no se había mantenido actualizada. La presencia de información actualizada podría resultar esencial para una respuesta rápida y eficaz ante una situación de crisis.

En cuanto a los controles fronterizos, las medidas de ciberseguridad no eran adecuadas ni tenían garantías de futuro. En primer lugar, los sistemas de control fronterizo importantes tenían que recibir una aprobación formal antes de ponerse en funcionamiento, a fin de asegurar la implementación de todas las medidas de ciberseguridad. Hallamos que dos de los tres sistemas estaban operativos sin dicha aprobación, lo que significaba que no existía garantía alguna de que contaran con las medidas de seguridad necesarias. En segundo lugar, había un Centro operativo, pero ninguno de los sistemas estaba directamente conectado al mismo. Aunque había infraestructuras genéricas vinculadas al Centro, esto seguía planteando el riesgo de que los ciberataques pasaran inadvertidos o se detectaran demasiado tarde. En tercer lugar, no se llevaban a cabo periódicamente pruebas de seguridad. De hecho, solo uno de los tres sistemas había sido objeto de pruebas en el pasado, y solo de forma limitada. Por último, al igual que en la primera auditoría, no se había elaborado un escenario específico para una crisis provocada por un ciberataque.

Durante la prueba de seguridad de uno de los sistemas que nunca se habían sometido a ensayos antes, los piratas informáticos éticos encontraron una serie de vulnerabilidades. Estas vulnerabilidades se podrían explotar en combinación con un intruso malicioso para lanzar un ciberataque y acceder, copiar e incluso manipular la información del sistema. Estos resultados demuestran la importancia de unas pruebas periódicas de la seguridad.

Las constataciones son preocupantes en razón de la automatización en curso de los procesos fronterizos. En el futuro próximo, un creciente número de sistemas de control fronterizo tratarán cada vez más datos empleando cada vez más conexiones. Esto incrementa el riesgo de ciberataques, por lo que el enfoque adoptado no presentaba garantías de futuro.

Conclusiones

En el supuesto de las estructuras hídricas, algunos elementos clave impedían al auditado tomar las medidas de ciberseguridad finales. Por ejemplo, no estaba claro cuál era el nivel de la amenaza, lo que dificultaba valorar si las medidas adoptadas y el presupuesto asignado eran suficientes o no. Además, el departamento central responsable de la ciberseguridad carecía de un mandato para implementar las medidas de ciberseguridad necesarias en las estructuras hídricas descentralizadas. En este ámbito, se siguieron las recomendaciones de la auditoría, lo que ayudó a la organización a seguir adelante.

En cuanto a los controles fronterizos, no había un motivo claro del nivel insuficiente de seguridad cibernética. La investigación de la auditoría halló procedimientos y políticas de ciberseguridad completos y detallados, así como unos conocimientos técnicos suficientes y empleados cualificados. Por lo tanto, las recomendaciones de la auditoría se centraron principalmente en garantizar que se hubieran adoptado efectivamente todas las medidas posibles.

Ambas auditorías suscitaron un elevado interés en el Parlamento y los medios de comunicación. Las auditorías mejoraron la sensibilización sobre ciberseguridad en relación con las infraestructuras vitales y les brindaron a los auditados información práctica sobre cómo mejorar su ciberseguridad. La estrecha cooperación con el auditado resultó esencial para comprender plenamente su situación y abordar los riesgos de investigar y poner a prueba la ciberseguridad.

En esta serie, hay también prevista una tercera auditoría. Por añadidura, el grado de seguridad de la información del Gobierno nacional neerlandés es un elemento clave del ciclo anual de auditorías de conformidad. Con el paso de los años, la EFS neerlandesa ha observado que muchos ministerios tienen deficiencias en cuanto a las medidas de seguridad de la información. El Tribunal de Cuentas está aplicando actualmente la experiencia atesorada en sus auditorías de ciberseguridad para ampliar su perspectiva sobre auditoría de seguridad de la información, mirando más allá de los documentos y las políticas y poniendo a prueba la eficacia real de las medidas.

Otros informes en este ámbito

Título del informe:	Capítulo 3 de «*Staat van de rijksverantwoording 2019*»
Enlace al informe:	Informe (versión en neerlandés)
Fecha de publicación:	2020

Título del informe:	Enfoque en el trabajo digital en el hogar
Enlace al informe:	Informe (versión en neerlandés)
Fecha de publicación:	2020

Polonia
Najwyższa Izba Kontroli

Garantizar la seguridad del funcionamiento de los sistemas informáticos empleados para desempeñar tareas públicas

Fecha de publicación: 2016

Enlace al informe: Informe (versión en polaco)

Tipo y período de auditoría

Tipo de auditoría: De conformidad

Período auditado: 2014-2015

Resumen del informe

Tema de la auditoría

La finalidad de la auditoría era evaluar si los datos recogidos en los sistemas diseñados para prestar importantes servicios públicos eran seguros en las unidades auditadas. La auditoría abarcó seis instituciones seleccionadas, responsables de tareas públicas significativas. Tras el análisis, se seleccionó un sistema informático esencial en cada una de las instituciones, para examinarlo a continuación en detalle. Se aplicó a la auditoría la versión 4.1 del método COBIT (objetivos de control para la información y tecnologías afines).

Esta auditoría se llevó a cabo tras la realizada en 2015 sobre el rendimiento de las tareas de ciberseguridad de los «organismos públicos» en Polonia[67], cuyas conclusiones detectaron problemas sistémicos. Entre otras cosas, la auditoría de 2016 demostró que la Administración del Estado no había tomado hasta entonces medidas para garantizar la seguridad informática a escala nacional. Se concluyó que las actividades de las entidades públicas relativas a la protección del ciberespacio se habían acometido de manera fragmentada y carecían de un enfoque sistemático. En

[67] https://www.nik.gov.pl/kontrole/P/14/043/

ausencia de disposiciones centralizadas con el fin de garantizar unas condiciones de seguridad concretas para sistemas informáticos específicos, esenciales para el funcionamiento del Estado, la auditoría se dirigió a examinar si las instituciones que administraban los sistemas informáticos utilizados para prestar importantes servicios públicos garantizaban que dichos servicios podían prestarse de forma segura.

Otra auditoría de los sistemas de ciberseguridad titulada «La ciberseguridad en Polonia» fue aprobada en 2019, si bien sus constataciones son confidenciales.

Preguntas de auditoría

Los objetivos secundarios se dividieron entre dos ámbitos de evaluación, buscando respuestas a cuestiones específicas.

En el área del apoyo a la seguridad informática, la auditoría examinó a escala de toda la organización, entre otras cosas, si:

- se aplicaba una gestión de la seguridad informática;
- se habían instaurado planes para garantizar la seguridad informática;
- la seguridad informática era objeto de pruebas, supervisión y vigilancia;
- se habían definido incidentes de seguridad informática;
- las tecnologías de la información se gestionaban mediante claves criptográficas;
- se había implementado una protección frente a los programas maliciosos, un sistema destinado a su detección y los correspondientes parches;
- se había garantizado la seguridad de la red.

En el ámbito del apoyo a la seguridad, la auditoría examinó a escala de los sistemas seleccionados, entre otras cosas, si:

- se gestionaban la identidad y las cuentas de los usuarios;
- las tecnologías de seguridad y los datos sensibles estaban protegidos.

Constataciones y conclusiones

El grado de preparación e implementación del sistema de seguridad de la información no aportaba un nivel de seguridad aceptable para los datos recogidos en los sistemas

informáticos destinados a prestar importantes servicios públicos. Los procesos de seguridad de la información se ejecutaban de forma desordenada e intuitiva ante la ausencia de procedimientos establecidos. De las seis unidades auditadas, solo una había implementado el sistema de seguridad de la información, y cabe señalar que su funcionamiento también contaba con defectos notables. En todas las unidades auditadas, salvo una, la labor para asegurar unas condiciones adecuadas de seguridad para la información tratada en los sistemas informáticos no había alcanzado el nivel adecuado, ya que, al haberse emprendido en tiempos recientes, estaba en una fase preliminar, que además implicaba la redacción de los fundamentos formales necesarios. Se había apoyado en disposiciones simplificadas o informales basadas en buenas prácticas o en la experiencia del personal informático hasta ese momento.

De conformidad con la metodología COBIT 4.1, la madurez del proceso de gestión de la seguridad de la información en las diversas unidades auditadas oscilaba entre (1) inicial/*ad hoc* y (3) definido, en una escala del cero al cinco en la que el cinco es el máximo.

La responsabilidad de garantizar la seguridad informática en las unidades auditadas recaía en el coordinador de seguridad, quien, en la práctica, no obstante, carecía de competencia para gestionar todo el proceso. A menudo, era solo una persona quien ejecutaba las tareas implicadas. Aunque se habían formado equipos de especialistas o se habían celebrado acuerdos con contratistas externos, no se había acometido el análisis necesario para establecer si los servicios prestados satisfacían las necesidades de seguridad de una unidad. La perspectiva de las unidades auditadas acerca de la necesidad de garantizar la seguridad informática era fragmentada y limitada. La seguridad de los datos se consideraba principalmente la responsabilidad y el ámbito de actuación del departamento informático y no de todas las unidades organizativas con cometidos legales, lo que obstaculizaba en gran medida el desarrollo de unos sistemas de gestión de la seguridad informática coherentes en toda la institución.

Al comparar la calidad de la manera en que se cumplían las obligaciones para garantizar la seguridad de la información, tanto con respecto a las organizaciones en su conjunto como en relación con los sistemas seleccionados, está claro que la calidad de la implementación era mayor en el segundo caso. Tal extremo puede deberse al impacto que tenían los conocimientos prácticos y la implicación de personal técnico de nivel medio en la garantía de la seguridad, el mayor uso dentro de la Administración pública de sistemas informáticos comerciales basados en normas del mercado y unas soluciones avanzadas de garantía de la seguridad. Mediante la aplicación de dichas soluciones, la experiencia en el pasado y las buenas prácticas, fue posible mantener un

cierto grado de seguridad en el funcionamiento de los diversos sistemas en condiciones de recursos limitados, deficiencias organizativas o normativas «disfuncionales». Sin embargo, esta no puede ser la solución objetivo, puesto que, en tiempos de un incremento dinámico en el nivel de amenazas, la seguridad de los sistemas informáticos no se puede basar en medidas gestionadas de forma desordenada y encaminadas solo a superar las dificultades inmediatas.

Conclusiones de la auditoría

Se deben desarrollar e implementar a escala centralizada recomendaciones y requisitos generales de seguridad informática, aplicables a todas las entidades públicas. Se necesita una solución sistémica gracias a la cual se divulguen los resultados de las auditorías de seguridad informática de una manera que permita a los ciudadanos acceder a la información sobre las actividades de las entidades públicas, a la vez que se mantiene restringido el acceso a los conocimientos sobre las medidas y los métodos empleados para garantizar la seguridad de la información tratada.

Otros informes en este ámbito

Título del informe:	Gestión de la seguridad de la información por parte de las autoridades regionales
Enlace al informe:	Informe (versión en polaco)
Fecha de publicación:	2019

Título del informe:	Ciberseguridad en Polonia (información clasificada)
Enlace al informe:	*No accesible al público*
Fecha de aprobación:	2019

Título del informe:	Garantía de la seguridad de los sistemas informáticos por parte de las autoridades regionales en el voivodato de Podlasie
Enlace al informe:	Informe (versión en polaco)
Fecha de publicación:	2018

Título del informe:	Prevención y lucha contra el ciberacoso a niños y jóvenes
Enlace al informe:	Informe (versión en polaco)
Fecha de publicación:	2017

Título del informe:	Actuación de los organismos públicos en relación con la ciberseguridad en Polonia
Enlace al informe:	Informe (versión en polaco)
Fecha de publicación:	2015

Título del informe:	Implementación de requisitos seleccionados en los sistemas de información, intercambio de información electrónica y Marco de Interoperabilidad Nacional sobre la base del ejemplo de algunos ayuntamientos y ciudades con estatus de distrito.
Enlace al informe:	Informe (versión en polaco)
Fecha de publicación:	2015

Portugal
Tribunal de Contas

Auditoría sobre el pasaporte electrónico portugués

Fecha de publicación: 2014

Enlace al informe: Informe (versión en portugués)

Tipo y período de auditoría

Tipo de auditoría: Auditoría de gestión

Período auditado: 2013

Resumen del informe

Tema de la auditoría

La auditoría operativa del pasaporte electrónico portugués (PEP) estaba orientada a la eficacia de los sistemas de información que apoyan su concesión, expedición y utilización, en especial en el control automatizado de pasajeros mediante la lectura de datos biométricos en las fronteras de Portugal[68].

Los principales objetivos de la auditoría fueron:

- Verificar el cumplimiento del Derecho nacional y de la Unión y las normas y directrices internacionales para la concesión, la expedición y la utilización del PEP, incluida la conformidad del marco jurídico nacional;
- Examinar la eficacia de los procesos clave asociados al ciclo de vida del PEP, en especial los relacionados con su concesión, expedición y uso;

[68] Nos referimos a los procedimientos automatizados de control fronterizo en Frontex (Agencia Europea de la Guardia de Fronteras y Costas).

- Examinar aspectos críticos del rendimiento de los sistemas de información, en especial el cumplimiento de los requisitos de seguridad relativos a los sistemas de información del PEP (SIPEP).

Entre los factores de riesgo clave se contaban:

- la pérdida o el robo de activos físicos o información electrónica;
- la utilización indebida de información confidencial;
- el riesgo de cumplimiento (la disconformidad con los requisitos jurídicos y normativos).

Período de auditoría: del 1 de enero de 2013 al 31 de diciembre de 2013 (ampliable en su caso a ejercicios anteriores o posteriores).

Constataciones y conclusiones

El pasaporte electrónico portugués (PEP) presenta tres categorías: ordinarios[69], diplomáticos o especiales. Existe también un pasaporte para no nacionales, que otorga menos privilegios.

El sistema de concesión tiene varias aplicaciones, entidades de recogida de datos y organismos de concesión, pero solo un expedidor (que incorpora la fabricación, la personalización y la entrega).

En este proceso hay varias entidades participantes (entidades PEP). Los siguientes organismos recogen datos y conceden pasaportes:

- Portugal continental: el Serviço de Estrangeiros e Fronteiras (SEF)[70] y los servicios registrales del Instituto dos Registos e do Notariado (IRN)[71];

[69] Alrededor del 99 % del total.

[70] Servicio de Extranjería y Fronteras.

[71] Instituto de Registros y Notariado (solo recepción).

- Regiones autónomas de las Azores[72] y de Madeira: servicios prestados por la correspondiente *Vice-Presidência do Governo Regional*[73]; en el extranjero: los consulados portugueses;

- La Imprensa Nacional – Casa da Moeda, S.A. (INCM)[74] expide y entrega los pasaportes.

Los principales procesos se ejecutan sobre todo en el SIPEP (sistema de solicitud de gestión centralizada para la expedición de los pasaportes portugueses). El SIPEP hace posible el registro, el almacenamiento, el tratamiento, la validación y la entrega de la información necesaria para la concesión del PEP, activa el proceso de personalización llevado a cabo por la INCM y garantiza la interconexión con otras aplicaciones del sistema, coordinando a todas las entidades PEP involucradas en el registro físico y logístico de los datos recogidos.

Las entidades PEP cuentan con una estructura organizativa que les permite alcanzar los objetivos legales asociados al PEP. El sistema se sigue basando en gran medida en los recursos humanos en las etapas de solicitud y recogida de datos. Sin embargo, el SIPEP incluye varias funciones de tratamiento y controles de validación automáticos.

Los procedimientos, algunos de los cuales pueden llevarse a cabo de manera autónoma, sin intervención humana, garantizan las funciones de control y la manipulación de los datos. Por ello, el SIPEP tiene un impacto significativo en cuanto a la organización y al sistema de información, en particular en lo concerniente a: i) la comprensión y la definición de las normas, los procesos y los datos necesarios, y ii) la definición de los propios requisitos del sistema de información.

La eficiencia y la eficacia del proceso de recogida de datos están garantizadas por la interacción del SIPEP con otros sistemas de información[75], de acuerdo con la normativa legal.

---

[72] Y los puntos de servicios de la *Agência para a Modernização e Qualidade do Serviço ao Cidadão, I. P. (RIAC)* [Agencia para la Modernización y la Calidad del Servicio al Ciudadano, instituto público (solo recepción)].

[73] Vicepresidencia del Gobierno regional.

[74] Fábrica Nacional de Moneda y Timbre, empresa pública.

[75] A saber: Sistema de Información Integrado del SEF (SIISEF); parte nacional del Sistema de Información de Schengen (NSIS); base de datos de identificación civil, base de datos de antecedentes penales.

Aunque no está exhaustivamente documentado, se ha establecido un marco de control global para las actividades informáticas (gobernanza, desarrollo y adquisición, operaciones informáticas, continuidad de las actividades y recuperación en caso de catástrofes, seguridad de la información) que garantiza el desarrollo, el funcionamiento, la gestión y el mantenimiento del sistema SIPEP.

Indicadores de actividad (2013):

- se concedieron unos 500 000 PEP, de los cuales alrededor del 63 % por el SEF, el 33 % por los consulados portugueses y el 4 % por los Gobiernos regionales;
- los ingresos por la expedición de los PEP ascendieron en total a unos 37 millones de euros, principalmente de la INCM (43 %), el SEF (32 %) y el *Ministério dos Negócios Estrangeiros (MNE)*[76] (17 %).

En 2013, las pruebas realizadas en el SIPEP no confirmaban el cumplimiento del plazo de entrega máximo legalmente establecido (desde la fecha de la solicitud hasta la disponibilidad del PEP para su recogida en el punto de entrega), ya que la fecha de entrega efectiva en el punto de entrega no se registraba siempre de manera oportuna.

El SEF, el MNE, la RIAC y la INCM efectuaron inversiones relativas a la adquisición de equipos para la recogida de datos biométricos y firmas (terminales) y equipos para los procedimientos automatizados de control fronterizo, la adquisición y el mantenimiento de sistemas y servicios informáticos y asistencia técnica por valor de 11 millones de euros.

Antes del PEP, el precio del pasaporte (no biométrico) de la República Portuguesa ascendía a 22,44 euros; en 2006, el PEP (biométrico) ordinario tenía un precio de 60 euros, que se incrementó hasta los 65 euros en 2011.

Solicitudes de PEP

Las solicitudes de PEP son tratadas en persona por los servicios competentes, que reciben los documentos de la solicitud, recogen los datos personales y biométricos de los solicitantes, cobran las tasas y, con posterioridad, entregan el PEP expedido.

[76] Ministerio de Asuntos Exteriores.

El sistema subyacente (SIPEP) valida la corrección y la calidad de los datos a través de controles virtuales y referencias cruzadas con otros sistemas de información, como la Base de Datos de Identificación Civil, a fin de garantizar que la solicitud sea conforme y adecuada para la concesión y la expedición de PEP.

Los correspondientes cambios de situación se almacenan en archivos de registro, garantizando así la posibilidad de auditoría, la integridad y la aceptación de las transacciones.

La transmisión de datos entre los organismos encargados de su recogida (en Portugal y en el extranjero) y el SEF tiene lugar a través de una VPN (red privada virtual), implantada con arreglo a la gestión de los accesos y de conformidad con las credenciales controladas por el SEF[77].

La solicitud del PEP ordinario se procesa de una manera diferente cuando la presentan ciudadanos cuyos derechos son limitados o están restringidos, como: i) las personas que no pueden ejercer sus derechos (menores, discapacitados o personas inhabilitadas); ii) personas excluidas judicialmente o por la Policía (antecedentes penales, litigios pendientes o confiscación de documentos), y iii) cuando el solicitante de un segundo PEP invoca un interés nacional o legítimo.

Concesión del PEP

La decisión de conceder el PEP ordinario puede:

- Ser automática: aprobación automática por parte del sistema de solicitudes del SIPEP tras la validación de la identidad del solicitante y la ausencia de antecedentes penales (a través de un control cruzado con las bases de datos de identificación civil y de antecedentes penales del IRN) y litigios pendientes. Solo tiene lugar en el SEF, para solicitudes del PEP en el continente[78].

[77] El SIPEP es accesible (a través de la web) a escala regional, nacional e internacional para los servicios ubicados en las regiones autónomas de las Azores y de Madeira, en el continente y en el extranjero (consulados portugueses).

[78] Esta es una funcionalidad automatizada del sistema de solicitudes del SIPEP para aceptar (denominado internamente «autorizar») una solicitud (excepto en un segundo PEP) de un ciudadano mayor de edad, con un documento válido de identidad, sin litigios pendientes y que no esté excluido o inhabilitado. Los PEP ordinarios concedidos por el SEF, alrededor del 60 % del total, estaban cubiertos por procedimientos de validación y decisiones de

- Someterse a la aceptación o la autorización individual de otras entidades (Gobiernos regionales y oficinas consulares) o, en el caso del SEF, a requisitos no abarcados por la concesión automática[79].

Expedición del PEP

La expedición del PEP, que abarca la producción, la personalización y la entrega, es competencia de la INCM. Cuando la entrega del PEP se registra en el SIPEP, el estatus del pasaporte cambia a «Válido».

Los precios del PEP difieren en función del nivel de servicio requerido. Para medir el nivel de servicio, el SIPEP tiene que considerar la fecha de entrega efectiva del PEP,

que se encomienda a un servicio de transporte externalizado.

Anulación del PEP

Cuando un solicitante entrega un PEP todavía válido, debe desactivarse para impedir su nueva utilización, lo que corresponde al registro del estatus del pasaporte como «inutilizable» en el sistema de solicitudes SIPEP.

concesión automáticos y el resto eran objeto de análisis y aprobación por parte de la *Direção Central de Imigração e Documentação (DCID)*.

[79] En especial en los casos de solicitantes que no puedan ejercer sus derechos (menores, discapacitados o personas inhabilitadas), impedidos judicialmente o por la policía o, en el caso de un segundo PEP, cuya solicitud es estudiada caso por caso por la DCID.

Finlandia
Valtiontalouden tarkastusvirasto

Medidas de ciberprotección

Fecha de publicación: 2017

Enlace al informe: Informe (versión en finlandés)

Tipo y período de auditoría

Tipo de auditoría: Auditoría de gestión

Período auditado: 2016-2017

Resumen del informe

Tema de la auditoría

La finalidad de la auditoría era investigar si la ciberprotección en el Gobierno central se había dispuesto de la manera más eficaz y rentable posible. La auditoría se centró en cómo se organizaba y gestionaba la ciberseguridad del Gobierno central. Los resultados de la auditoría se podrían utilizar para desarrollar la eficacia y la eficiencia de la ciberseguridad en el Gobierno central. La auditoría se llevó a cabo desde el 22 de septiembre de 2016 hasta el 4 de septiembre de 2017. Se efectuó un seguimiento en otoño de 2019, en el que la Oficina Nacional de Auditoría examinó las medidas adoptadas a partir de las conclusiones y las recomendaciones de la auditoría.

Entre las entidades auditadas se incluyeron las autoridades encargadas de regular la protección cibernética en el Gobierno central (la Oficina del Primer Ministro, el Ministerio de Hacienda y el Ministerio de Transporte y Comunicaciones), así como las autoridades responsables de las tareas de ciberprotección y los servicios informáticos centralizados del Gobierno del Estado (el Centro Nacional de Ciberseguridad de la Agencia de Transportes y Comunicaciones de Finlandia, el Centro Valtori de TIC del Gobierno y la Agencia de Servicios de Datos Digitales y de Población). La eficacia de la orientación se evaluó también examinando las unidades del Gobierno central que prestaban servicios electrónicos (la Agencia de Servicios de Datos Digitales y de

Población, la Agencia de Transportes y Comunicaciones de Finlandia Traficom, la Oficina Administrativa Nacional de Ejecución y su supervisor, el Ministerio de Justicia, y el Centro de Servicios de TIC del Ministerio de Justicia).

Preguntas de auditoría

Las siguientes preguntas de auditoría se utilizaron en la auditoría de la organización de la ciberseguridad:

- Al organizar la ciberseguridad, ¿atribuyó la entidad auditada al aspecto económico una relevancia suficiente?
- ¿El conocimiento de la situación en materia de ciberseguridad de la entidad auditada respalda la ciberseguridad de los sistemas?
- ¿Es suficiente la capacidad de la entidad auditada para responder a las ciberviolaciones?

El tema de auditoría de las medidas de ciberprotección formaba parte de la temática de la auditoría «Garantizar la fiabilidad operativa de la sociedad de la información» del plan de auditoría 2016-2020 de la Oficina Nacional de Auditoría de Finlandia. Desde el punto de vista de la importancia para las finanzas del Gobierno central, la temática de la auditoría puede encontrar justificación en las desventajas relacionadas con las interrupciones del servicio y las violaciones de la seguridad de los datos, así como en los efectos negativos de una ciberseguridad deficiente en las actividades comerciales. Esta auditoría se llevó a cabo en paralelo con la auditoría «Dirección de la fiabilidad operativa de los servicios electrónicos», que pertenece al mismo tema. El material de auditoría clave consistió en documentos y entrevistas con las autoridades responsables de la actividad en cuestión.

Constataciones y conclusiones

La estrategia de ciberseguridad de Finlandia define los objetivos y las políticas clave para dar respuesta a los desafíos que entraña el ciberespacio y garantizar su funcionamiento. Se han acometido esfuerzos por instaurar la estrategia de ciberseguridad a través de un programa de implementación, cuyo progreso se evalúa anualmente. El Comité de Seguridad es un organismo de cooperación dentro del Ministerio de Defensa que supervisa y coordina la aplicación de la estrategia de ciberseguridad.

La organización eficaz de la ciberseguridad consiste en la gestión de riesgos, que, para un correcto funcionamiento, requiere unas estructuras y disposiciones de gestión eficaces que integren dicha gestión en las operaciones a todos los niveles de la organización. Como muchos otros países, Finlandia y su Gobierno central no son autosuficientes en recursos de protección cibernética. Con el tiempo, la legislación de la Unión Europea ha ido aumentando y ha pasado a ser cada vez más vinculante. En el Gobierno finlandés, la responsabilidad de la ciberprotección está descentralizada y cada organismo estatal es responsable de su propia ciberseguridad. En el Gobierno central, la asignación de responsabilidades respecto de la naturaleza, del alcance y de la implementación de posibles ciberviolaciones es compleja.

Debido a esta complejidad, la respuesta a una anomalía podría ser demasiado lenta, y la escasa financiación ha limitado la implementación de la estrategia de ciberseguridad de Finlandia. Sobre la base de las constataciones de la auditoría, la Oficina Nacional de Auditoría llegó a las conclusiones siguientes e hizo las recomendaciones siguientes en relación con la organización de la ciberseguridad en el Gobierno central:

La gestión operativa de las violaciones generalizadas de la ciberseguridad no estaba definida

Planificar la gestión operativa de las violaciones generalizadas de la ciberseguridad y el reparto de las correspondientes responsabilidades podrían permitir reacciones más rápidas, una coordinación adecuada y la asignación de recursos para las contramedidas. En el actual modelo operativo, cada agencia es responsable de su propia protección cibernética. Sin embargo, no se dispone de suficientes conocimientos técnicos al respecto, lo que impide la generación de ciberprotección, ya sea internamente o mediante su externalización.

No se alcanzaron algunos objetivos estratégicos de ciberseguridad

El programa de implementación de la estrategia de ciberseguridad finlandesa había mejorado la ciberprotección. Sin embargo, no se habían logrado algunos de los objetivos del primer programa de implementación debido al distinto nivel de compromiso con las acciones, que no se podía mejorar de manera centralizada. El nuevo programa de implementación solo incluía las acciones para las que las autoridades competentes y otros agentes hubieran expresado su compromiso. El compromiso y los recursos disponibles eran mutuamente dependientes entre sí.

No estaba clara la idoneidad de las soluciones de financiación de la protección cibernética

Las diferencias en el desarrollo de la ciberprotección se debían en parte a las distintas cantidades de recursos de los que disponían las organizaciones. En la normativa sobre la preparación del presupuesto estatal o en el propio proceso de preparación no se detectaron procedimientos para garantizar que los fondos se asignaran a los objetivos de ciberprotección más importantes. Las agencias y las instituciones presupuestaban las partidas para ciberseguridad como una parte no especificada de sus gastos de funcionamiento. Las medidas descritas en la estrategia de ciberseguridad de Finlandia se implementaban solo en la medida en que lo permitían dichas partidas.

La ciberprotección se debe tener en cuenta también en los cambios de la organización de las TIC

Los cambios en la organización de las TIC del Gobierno central habían influido en las medidas de ciberprotección. El desarrollo de una ciberseguridad centralizada por Valtori había resultado difícil. Había deficiencias en la evaluación de la adecuación de los procedimientos prácticos de ciberprotección y en la implementación de nuevas medidas.

Se debe mejorar el conocimiento de la situación de las operaciones de ciberseguridad

El Centro de Ciberseguridad mantenía un conocimiento en todo el país acerca de la situación de la ciberseguridad. En el momento de la auditoría, no existía la obligación de informar sobre violaciones de la ciberseguridad a dicho Centro. Obligar a las organizaciones gubernamentales a denunciar las violaciones mejoraría la situación, ya que ampliaría la cobertura de los procedimientos centralizados de detección de ciberviolaciones.

Con arreglo a lo que antecede, la Oficina Nacional de Auditoría recomienda que el Ministerio de Hacienda defina e implemente un modelo completo de gestión operativa en caso de incidentes de ciberseguridad en los servicios de TIC del Gobierno central. Además, el Ministerio de Hacienda debería averiguar cómo tener en cuenta la ciberseguridad de los servicios en la financiación de servicios a lo largo de su ciclo de vida y mejorar el conocimiento sobre la situación operativa ordenando a las autoridades que comuniquen las ciberviolaciones al Centro de Ciberseguridad. Se recomendó que Valtori mejorara la implementación, la evaluación y el desarrollo de procedimientos de ciberseguridad y la detección de ciberviolaciones.

La auditoría de seguimiento examinó cómo se habían aplicado las recomendaciones facilitadas durante la auditoría. La Oficina de Auditoría consideró que el Ministerio de Hacienda, como autoridad competente para la implementación de las recomendaciones, no había tomado medidas suficientes en respuesta a las recomendaciones realizadas. Sin embargo, la ciberseguridad se había reforzado en Finlandia también a través de medidas adoptadas por otras autoridades diferentes del Ministerio de Hacienda. Se estaba produciendo un cambio en la gestión estratégica de la ciberseguridad hacia el modelo directivo en la materia. En el proyecto de presupuesto para 2020, el Gobierno aumentó las partidas para las autoridades de la Administración central que desempeñan una función clave en el fortalecimiento de la ciberseguridad. Por añadidura, Valtori estaba adoptando medidas en consonancia con la recomendación de la Oficina Nacional de Auditoría. En conclusión, la Oficina Nacional de Auditoría señaló que era necesaria una auditoría de seguimiento debido a las recomendaciones pendientes de aplicación y que una auditoría totalmente nueva en este ámbito estaba justificada por los cambios en curso en las medidas de ciberseguridad y el entorno operativo digital y los correspondientes riesgos, así como por la importancia de la ciberseguridad para las finanzas del Gobierno central y la sociedad.

Suecia
Riksrevisionen

Sistemas informáticos obsoletos: un obstáculo para la digitalización efectiva

Fecha de publicación: 2019

Enlace al informe: Resumen del informe (versión en inglés)
Informe (versión en sueco)

Tipo y período de auditoría

Tipo de auditoría: Auditoría de gestión

Período auditado: 2018-2019

Resumen del informe

Tema de la auditoría

Los sistemas informáticos esenciales para la actividad, pero ya obsoletos, implican un gran riesgo de problemas de eficiencia, puesto que, en proporción, las organizaciones se ven obligadas a dedicar más recursos tan solo para mantener el sistema. Por tanto, hay buenas razones para asumir que los sistemas informáticos obsoletos implican un elevado riesgo de gestión de los fondos públicos de forma inapropiada. También conllevan una cierta anulación de la capacidad innovadora de un organismo en lo que se refiere al desarrollo de nuevos sistemas informáticos. Sin embargo, los sistemas informáticos obsoletos no solo comportan riesgos para las agencias individuales, sino que los problemas en una de ellas pueden acarrear graves consecuencias para su capacidad de coordinar sus operaciones con otra agencia o parte interesada privada. Los sistemas informáticos obsoletos también conllevan riesgos desde una perspectiva de la seguridad de la información.

Definición del objeto principal de la auditoría/Preguntas de auditoría/Contexto

La finalidad de la auditoría era examinar la incidencia de los sistemas informáticos obsoletos en la Administración del Estado y evaluar si las autoridades y el Gobierno habían tomado medidas adecuadas para evitar que dichos sistemas se convirtieran en un obstáculo para la digitalización efectiva. Las preguntas de auditoría planteadas fueron:

- ¿Han tomado las autoridades medidas adecuadas para abordar los problemas asociados a los sistemas informáticos obsoletos?
- ¿Ha tomado el Gobierno medidas adecuadas para abordar los problemas asociados a los sistemas informáticos obsoletos?

Constataciones y conclusiones

- La auditoría reveló que había sistemas informáticos obsoletos en un gran número de agencias gubernamentales. En muchas de ellas, además, uno o varios sistemas informáticos esenciales para su actividad estaban obsoletos. Según los datos de los que dispone la Oficina sueca, se trata de información nueva y nadie antes era consciente del alcance del problema en la Administración del Estado. Alrededor del 80 % de las agencias indicó que tenía dificultades para mantener el nivel de seguridad de la información en uno o varios de los sistemas esenciales para su actividad. Más de una de cada diez autoridades respondió que esto era aplicable a todos los sistemas, o a la mayoría de ellos.
- Una proporción considerable de las agencias examinadas no tenía un enfoque correcto con respecto al desarrollo y la administración del apoyo informático. No utilizaban las herramientas existentes para el desarrollo operativo a fin de determinar cómo sacar el máximo provecho del apoyo informático para lograr los objetivos de las operaciones centrales. Así, gran parte de las agencias auditadas carecía de una perspectiva general sobre cómo estaban vinculados los procesos operativos, las estrategias y los sistemas. Esto, a su vez, significaba que se enfrentaban a dificultades para analizar y comprender de qué manera afectaban los cambios a los objetivos de la organización y, en consecuencia, era más complicado definir la situación deseable en el futuro.
- Más de la mitad de las autoridades indicó que no existía un modelo aprobado para gestionar y tomar decisiones sobre sus sistemas informáticos desde la fase de desarrollo hasta su desmantelamiento, denominado generalmente gestión del

ciclo de vida. De conformidad con la Oficina sueca, tal extremo indicaba que la gestión del ciclo de vida no se acometía de una manera estructurada y metódica. También había deficiencias en la labor de análisis de riesgos y en la capacidad para desglosar los costes informáticos hasta el nivel de detalle necesario para adoptar decisiones acertadas.

- Casi el 60 % de las autoridades carecía de planes para el ciclo de vida del desarrollo de los sistemas, con la excepción de uno o unos pocos sistemas esenciales para la actividad. La ausencia de planes para el ciclo de vida u otra documentación programática en numerosas agencias, en combinación con las deficiencias en la gestión del ciclo de vida llevada a cabo en la práctica, conllevaba que no se pudiera considerar que las agencias, en general, hubieran desarrollado una postura consciente y explícita en cuanto a sus sistemas informáticos.

- La Oficina sueca considera que los ministerios implicados y, por ende, también el Gobierno, carecían de conocimientos suficientes tanto sobre la incidencia como sobre las consecuencias de los sistemas informáticos obsoletos.

La conclusión general fue que, en el momento de la auditoría, la mayoría de las agencias no había logrado realmente afrontar con eficacia los problemas dimanantes de unos sistemas informáticos obsoletos. La Oficina sueca consideró que el problema era tan grave y estaba tan extendido que suponía un obstáculo para continuar con una digitalización eficiente de la Administración estatal. La auditoría reveló asimismo que el Gobierno carecía de conocimientos sobre la existencia y las consecuencias de los problemas de los sistemas informáticos obsoletos. Por añadidura, el Gobierno no había tomado ninguna medida para abordar el problema de los sistemas informáticos obsoletos de una manera más directa. La valoración de la Oficina sueca fue por tanto que no se podía considerar que el Gobierno hubiera tomado las medidas suficientes para garantizar la mitigación o la subsanación de los problemas.

Otros informes en este ámbito

Título del informe:	Facilitar la constitución de una empresa: esfuerzos gubernamentales por promover un proceso digital (RiR 2019:14)
Enlace al informe:	Resumen del informe (versión en inglés) Informe (versión en sueco)
Fecha de publicación:	2019

Título del informe:	Digitalización de la Administración pública: una Administración más simple, transparente y eficaz (RiR 2016:14)
Enlace al informe:	Resumen del informe (versión en inglés) Informe (versión en sueco)
Fecha de publicación:	2016

Título del informe:	Trabajo en seguridad de la información en nueve agencias (RiR 2016:8)
Enlace al informe:	Resumen del informe (versión en inglés) Informe (versión en sueco)
Fecha de publicación:	2016

Título del informe:	Ciberdelincuencia: los policías y los fiscales pueden ser más eficientes (RiR 2015:21)
Enlace al informe:	Resumen del informe (versión en inglés) Informe (versión en sueco)
Fecha de publicación:	2015

Unión Europea
Tribunal de Cuentas Europeo

Documento informativo: Desafíos de una política eficaz de ciberseguridad

Fecha de publicación: 2018

Enlace al informe: Informe (versiones en 23 lenguas)

Tipo y período de auditoría

Tipo de auditoría: Análisis de políticas

Período auditado: De abril a septiembre de 2018

Resumen del informe

Tema del análisis

En el presente documento informativo, que no es un informe de auditoría, se presenta una visión general de la compleja política de ciberseguridad de la UE y se determinan los principales desafíos que plantea su aplicación eficaz. Trata sobre la seguridad de las redes y de la información, la ciberdelincuencia, la ciberdefensa y la desinformación.

El análisis del Tribunal se basó en una revisión de documentos oficiales y de acceso público, documentos de posición y estudios de terceros. El trabajo de campo se realizó entre abril y septiembre de 2018, y tuvo en cuenta la evolución hasta diciembre de 2018. El Tribunal completó su trabajo con una encuesta a las oficinas nacionales de auditoría de los Estados miembros y entrevistas con partes interesadas clave de instituciones de la UE y representantes del sector privado.

No existe ninguna definición normalizada de «ciberseguridad», pero, en líneas generales, se puede describir como el conjunto de garantías y medidas adoptadas para defender los sistemas de información y a sus usuarios frente a accesos no autorizados, ataques y daños para garantizar la confidencialidad, la integridad y la disponibilidad de los datos. La ciberseguridad consiste en prevenir y detectar ciberincidentes, así como responder ante los mismos y recuperarse de estos. Los incidentes pueden ser o no intencionados y consisten, por ejemplo, en acciones que van desde la divulgación

accidental de información hasta los ataques a empresas e infraestructuras críticas o el robo de datos personales, e incluso la injerencia en procesos democráticos.

La piedra angular de la política de la UE es la Estrategia de Ciberseguridad de 2013. Su objetivo es lograr que el entorno digital de la UE sea el más seguro del mundo, defendiendo al mismo tiempo los valores y las libertades fundamentales. Tiene cinco objetivos principales: i) aumentar la ciberresiliencia, ii) reducir la ciberdelincuencia, iii) desarrollar estrategias y capacidades de ciberdefensa, iv) desarrollar recursos tecnológicos e industriales de ciberseguridad, y v) crear una política internacional del ciberespacio de acuerdo con los valores esenciales de la UE.

Constataciones

Debido a la falta de datos fiables, fue difícil calcular el impacto de la falta de preparación ante un ciberataque. El impacto económico de la ciberdelincuencia se quintuplicó entre 2013 y 2017, y afecta a Gobiernos y a empresas, tanto grandes como pequeños por igual. El crecimiento previsto de las primas de seguros cibernéticos, que pasaron de 3 000 millones de euros en 2018 a 8 900 millones de euros en 2020, refleja esta tendencia. A pesar de que el 80 % de las empresas de la UE experimentó al menos un incidente de ciberseguridad en 2016, el conocimiento de los riesgos sigue siendo alarmantemente bajo. El 69 % de las empresas de la UE tiene un conocimiento nulo o limitado de su exposición a las amenazas cibernéticas, y el 60 % no ha calculado nunca las potenciales pérdidas económicas. Según una encuesta mundial, un tercio de las organizaciones preferiría pagar el rescate al pirata informático en vez de invertir en seguridad de la información.

Las constataciones del Tribunal fueron las siguientes:

- El ecosistema cibernético de la UE es complejo y multidimensional, e implica a numerosas partes interesadas. Agrupar todas las piezas que lo conforman constituye todo un desafío.

- El objetivo de la UE es convertirse en el entorno en línea más seguro del mundo. Lograrlo requiere esfuerzos significativos de todas las partes interesadas, así como una base financiera sólida y bien gestionada. Es difícil dar cifras, pero se estima que el gasto público de la UE en ciberseguridad oscila entre 1 000 y 2 000 millones de euros al año. En comparación, el Gobierno federal de EE. UU. tiene un presupuesto en la materia de unos 21 000 millones de dólares estadounidenses para 2019.

- La gobernanza de la seguridad de la información consiste en la creación de estructuras y políticas para garantizar la confidencialidad, la integridad y la disponibilidad de los datos. Es más que una mera cuestión técnica, por lo que exige un liderazgo eficaz, procesos sólidos y estrategias en consonancia con los objetivos de la organización.

- Los modelos de gobernanza de la ciberseguridad difieren entre los Estados miembros, y dentro de estos, las competencias en materia de ciberseguridad a menudo se reparten entre numerosas entidades. Estas diferencias podrían obstruir la cooperación necesaria para responder a incidentes transfronterizos de gran envergadura e intercambiar información sobre amenazas en el ámbito nacional, e incluso más a escala de la UE.

- Diseñar una respuesta eficaz a los ciberataques es fundamental para atajarlos cuanto antes. Es especialmente importante que los sectores críticos, los Estados miembros y las instituciones de la UE ofrezcan una respuesta rápida y coordinada. Una detección temprana es esencial para ello.

Recomendaciones

El análisis del Tribunal muestra que es necesario avanzar hacia una cultura del rendimiento con prácticas de evaluación integradas para garantizar una rendición de cuentas y una evaluación significativas. Quedan lagunas en la legislación, y la transposición de la legislación existente por los Estados miembros no se realiza de manera sistemática. Esto puede hacer más difícil que la legislación alcance su pleno potencial.

Otro desafío radica en ajustar los niveles de inversión a los objetivos estratégicos, que exige incrementar los niveles de inversión y el impacto. Esto es más complicado si la UE y sus Estados miembros carecen de una visión general clara del gasto de la Unión en ciberseguridad. También se informó de las restricciones en la asignación de recursos suficientes a las agencias pertinentes de la UE relacionadas con el ámbito cibernético, así como de las dificultades para atraer y mantener el talento.

Acrónimos y abreviaturas

AED: Agencia Europea de Defensa

APPc: Asociación público-privada contractual

CERT-UE: Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión Europea

COBIT: Objetivos de control para la información y tecnologías afines

COVID-19: Enfermedad por coronavirus de 2019

CSIRT: Equipo de respuesta a incidentes de seguridad informática

DDoS: Denegación de servicio distribuido

Directiva SRI: Directiva sobre seguridad de las redes y de la información

EC3: Centro Europeo de Ciberdelincuencia de Europol

EE. UU.: Estados Unidos de América

EFS: Entidades Fiscalizadoras Superiores

ENISA: Agencia de la Unión Europea para la Ciberseguridad

Europol: Agencia de la Unión Europea para la Cooperación Policial

Fondos EIE: Fondos Estructurales y de Inversión Europeos

FSI-P: Fondo de Seguridad Interior – Policía

ISACA: Asociación para la auditoría y el control de los sistemas de información

JERS: Junta Europea de Riesgo Sistémico

MCE: Mecanismo «Conectar Europa»

MERS: Síndrome respiratorio de Oriente Medio

MFP: Marco financiero plurianual

OTAN: Organización del Tratado del Atlántico Norte

PCSD: Política común de seguridad y defensa

PIB: Producto Interior Bruto

RGPD: Reglamento General de Protección de Datos

SARS: Síndrome respiratorio agudo grave

SEAE: Servicio Europeo de Acción Exterior

TI: Tecnologías de la información

TIC: Tecnologías de la información y de las comunicaciones

Tribunal: Tribunal de Cuentas Europeo

UE: Unión Europea

URL: Localizador uniforme de recursos

Glosario

5G: Norma tecnológica de quinta generación para las redes móviles de banda ancha, que las compañías de telefonía móvil comenzaron a desplegar en todo el mundo en 2019 y que se prevé que sustituya a las redes 4G que proporcionan conectividad a la mayoría de los teléfonos móviles actuales. La mayor velocidad se logra en parte mediante el empleo de ondas de radio a una frecuencia superior que las redes móviles anteriores.

Activo digital: Cualquier elemento existente en formato digital, propiedad de una persona física o jurídica y acompañado del derecho de uso (por ejemplo, imágenes, fotos, vídeos, archivos con texto, etc.).

***Adware*:** Programa informático malicioso que muestra anuncios publicitarios o ventanas desplegables con código para rastrear el comportamiento en línea de las víctimas.

Amenaza cibernética: Un acto malicioso con el objetivo de dañar o robar datos o perturbar la actividad digital en general.

Amenaza híbrida: Expresión de intento hostil que realizan los adversarios utilizando una combinación de técnicas de guerra convencionales y no convencionales (es decir, métodos militares, políticos, económicos y tecnológicos) en la persecución de sus objetivos.

Amenazas persistentes avanzadas: Ataque mediante el cual un usuario no autorizado consigue acceder a un sistema o una red y permanecer en su interior durante un período prolongado de tiempo sin ser detectado. Es especialmente peligroso para las empresas, ya que los piratas informáticos tienen un acceso continuo a datos societarios sensibles, aunque normalmente no causan daños a las redes o los equipos locales de la empresa. Su objetivo es el robo de datos.

Ataques basados en la web: Los usuarios definidos confían en que la información personal sensible que divulgan en el sitio web se mantendrá confidencial y segura. La intrusión (el ataque) puede conllevar la publicación de su información médica, de la seguridad social o de su tarjeta de crédito, lo que podría acarrear consecuencias potencialmente graves.

Bitcoin: Moneda digital o virtual creada en 2009 que utiliza la tecnología entre pares para facilitar pagos instantáneos.

Ciberataque: Intento de socavar o destruir la confidencialidad, la integridad y la disponibilidad de datos o de un sistema informático a través del ciberespacio.

Ciberdefensa: Subconjunto de la ciberseguridad destinado a defender el ciberespacio con medios militares u otros medios adecuados para lograr objetivos militares estratégicos.

Ciberdelincuencia: Distintas actividades delictivas en las que están implicados ordenadores y sistemas informáticos como herramienta u objetivo principal y que comprenden las siguientes: delitos tradicionales (por ejemplo, fraude, falsificación y usurpación de identidad), delitos relacionados con los contenidos (por ejemplo, distribución en línea de pornografía infantil o incitación al odio racial) y delitos exclusivos de ordenadores y sistemas de información (por ejemplo, ataques contra los sistemas de información, ataques de denegación de servicio, programas maliciosos o programas de secuestro).

Ciberdiplomacia: Empleo de recursos diplomáticos y desempeño de funciones diplomáticas para velar por los intereses nacionales con respecto al ciberespacio. La ejercen total o parcialmente los diplomáticos, que se reúnen en formatos bilaterales (como el diálogo entre EE. UU. y China) o en foros multilaterales (como en la ONU). Más allá del ámbito tradicional de la diplomacia, los diplomáticos interactúan asimismo con varios agentes privados, como los responsables de empresas de internet (como Facebook o Google), empresarios tecnológicos u organizaciones de la sociedad civil. La diplomacia puede implicar también dar voz a los sectores oprimidos en otros países gracias a la tecnología.

Ciberespacio: Entorno global intangible en el que se produce la comunicación en línea entre las personas, el programa informático y los servicios a través de redes informáticas y dispositivos tecnológicos.

Ciberespionaje: Acto o procedimiento para conseguir secretos e información, sin el permiso o el conocimiento de su titular, de personas físicas, competidores, rivales, grupos, Gobiernos y enemigos para granjearse así ventajas personales, económicas, políticas o militares utilizando internet, otras redes u ordenadores personales.

Ciberincidente: Incidente que perjudica o daña directa o indirectamente la resiliencia y la seguridad de un sistema informático y los datos que este trata, almacena o transmite.

Ciberresiliencia: Capacidad de prevenir los ciberataques y ciberincidentes, de prepararse para los mismos, de resistir y de recuperarse ante estos.

Ciberseguridad (ciberprotección): Conjunto de salvaguardias y medidas adoptadas para defender los sistemas informáticos y sus datos frente a accesos no autorizados,

ataques y daños con el fin de garantizar su disponibilidad, confidencialidad e integridad.

Cifrado: Transformación de información legible en código ilegible para su protección. Para leer la información, el usuario debe tener acceso a una clave secreta o contraseña.

Computación en la nube: Provisión de recursos informáticos y a demanda, como el almacenamiento, la potencia de computación o la capacidad de intercambio de datos, en internet a través de un alojamiento en servidores remotos.

Confidencialidad: Protección de información, datos o activos frente a un acceso no autorizado o su divulgación.

Contenido digital: Datos, como texto, sonido, imágenes o vídeo, almacenados en un formato digital.

Criptomoneda: Activo digital que se emite e intercambia utilizando técnicas de encriptación con independencia de un banco central y que es aceptado como medio de pago entre los miembros de una comunidad virtual.

Datos biométricos: Datos físicos (como las huellas dactilares y los ojos) o cálculos conductuales relacionados con las características humanas. La autenticación se utiliza en informática como forma de identificación y control del acceso.

Datos de acceso: Información sobre la actividad de inicio y cierre de sesión de un usuario para acceder a un servicio, como la hora, la fecha y la dirección IP.

Datos personales: Información relativa a un individuo identificable.

Denegación de servicio distribuido (DDoS): Ciberataque para impedir que los usuarios legítimos accedan a servicios o recursos en línea inundándolos de más solicitudes de las que pueden gestionar.

Desinformación: Información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población, y que puede causar un perjuicio público.

Digitalización: Proceso de convertir información a un formato digital, en el que esta se organiza en bits. El resultado es la representación de un objeto, una imagen, un sonido, un documento o una señal generando una serie de números que describen un conjunto discreto de puntos o muestras.

Disponibilidad: Garantizar el acceso oportuno y fiable a la información, así como su utilización.

Ecosistema cibernético: Comunidad compleja de dispositivos, datos, redes, personas, procesos y organizaciones en interacción, así como el entorno de procesos y tecnologías que influyen y apoyan estas interacciones.

Gusano: Programa informático malicioso independiente que se replica a fin de propagarse a otros ordenadores. A menudo utiliza una red informática para dicha propagación, basándose en los fallos de seguridad del ordenador objetivo para acceder al mismo.

Informática de alto rendimiento: Capacidad de tratar datos y llevar a cabo cálculos complejos a altas velocidades.

Infraestructura electoral: Abarca las bases de datos y los sistemas informáticos de campaña, la información sensible sobre los candidatos, el registro de los votantes y los sistemas de gestión.

Infraestructuras críticas: Recursos físicos, servicios e instalaciones cuya perturbación o destrucción tendría un grave impacto sobre el funcionamiento de la economía y la sociedad.

Ingeniería social: En seguridad de la información, manipulación psicológica para engañar a una persona con el fin de que realice una acción o divulgue información confidencial.

Instalaciones de empresas de servicios públicos: Cualquier poste, torre o conducciones aéreas o enterradas, cualquier otra estructura de soporte o apoyo y cualquier zanja, junto con sus correspondientes accesorios, susceptibles de ser utilizados para el suministro o la distribución de servicios eléctricos, telefónicos, telegráficos, de fibra óptica o cualquier otro servicio de señalización o similar.

Integridad: Protección frente a la modificación inapropiada o la destrucción de información y garantía de su autenticidad.

Inteligencia artificial: Simulación de inteligencia humana en máquinas programadas para pensar como los humanos e imitar sus acciones; cualquier máquina que muestre los rasgos asociados a una mente humana, como el aprendizaje y la resolución de problemas.

Internet de las cosas: Red de objetos cotidianos equipados con electrónica, programas informáticos y sensores para que puedan comunicar e intercambiar datos a través de internet.

Operador de servicios esenciales: Entidad pública o privada que presta un servicio esencial para el mantenimiento de actividades sociales y económicas cruciales.

Parcheado: Introducción de un conjunto de cambios en el programa informático para actualizarlo, repararlo o mejorarlo, incluida la reparación de vulnerabilidades de seguridad.

Pirata informático ético: Persona (experto en seguridad informática) que penetra en una red informática a fin de probar o evaluar su seguridad, sin intenciones maliciosas ni criminales.

Pirata informático: Persona que utiliza un ordenador, las redes u otras competencias para obtener un acceso no autorizado a datos, sistemas informáticos o redes.

Plataforma digital: Entorno para que se produzcan interacciones entre al menos dos grupos diferentes, siendo normalmente uno de ellos los proveedores y el otro los consumidores o el usuario. Puede tratarse del equipo físico o el sistema operativo, o incluso un navegador web y las correspondientes interfaces de programación de aplicaciones, u otros programas informáticos subyacentes, siempre que el código se ejecute con ellos.

Programa de secuestro: Programa informático malicioso que impide que las víctimas puedan acceder a un sistema informático o que hace ilegibles los archivos, generalmente mediante encriptación. Posteriormente, el atacante suele chantajear a la víctima negándose a restablecer el acceso hasta que no se pague un rescate.

Programa espía: Programa informático con un comportamiento malicioso dirigido a recabar información sobre una persona física o jurídica y enviarla a otra entidad de modo que el usuario resulte perjudicado; por ejemplo, violando su confidencialidad o poniendo en peligro la seguridad de su dispositivo.

Programa malicioso: *Software* malicioso. Programa informático diseñado para dañar ordenadores, servidores o redes.

Protocolo de escritorio remoto: Norma técnica (publicada por Microsoft) para utilizar a distancia un ordenador de sobremesa. Los usuarios de escritorios remotos pueden acceder a su ordenador de sobremesa, abrir y editar archivos y utilizar aplicaciones como si en realidad estuvieran ante dicho equipo.

Proveedor de servicios digitales: Cualquier persona física o jurídica que preste uno o varios de estos tres tipos de servicio digital: mercados en línea, motores de búsqueda o servicios de computación en la nube.

Sabotaje: Acción encaminada a destruir, dañar u obstruir deliberadamente, en especial para obtener ventajas políticas o militares.

Seguridad de la información: Conjunto de procesos y herramientas que protegen los datos físicos y digitales del acceso no autorizado, el uso, la divulgación, la perturbación, la modificación, el registro o la destrucción.

Seguridad de la red: Subconjunto de datos de protección de la ciberseguridad enviados a través de dispositivos en la misma red para garantizar que no se intercepta o modifica la información.

Sistema de información esencial: Cualquier sistema de información, existente o previsto, que se considere esencial para el funcionamiento eficiente y eficaz de una organización.

Suplantación de identidad: Práctica de enviar correos electrónicos supuestamente procedentes de una fuente fiable para engañar a sus destinatarios con el fin de que pulsen enlaces maliciosos o compartan información personal.

Tratamiento de datos: Realización de operaciones con datos, especialmente mediante un ordenador, para recuperar, transformar o clasificar información.

Troyano: Tipo de código o programa informático malicioso que parece legítimo pero que puede hacerse con el control de un ordenador. Un troyano está diseñado para dañar, perturbar, robar o, en general, infligir algún otro tipo de daño a datos o una red.

Vectorización de texto: Proceso de conversión de palabras, frases o documentos enteros en vectores numéricos para que los algoritmos de aprendizaje automático puedan utilizarlos.

Violación de la seguridad de los datos: Publicación intencionada o no de información confidencial o privada en un entorno no seguro.

Ponerse en contacto con la Unión Europea

En persona
En la Unión Europea existen cientos de centros de información Europe Direct. Puede encontrar la dirección del centro más cercano en: https://europa.eu/european-union/contact_es

Por teléfono o por correo electrónico
Europe Direct es un servicio que responde a sus preguntas sobre la Unión Europea. Puede acceder a este servicio:
— marcando el número de teléfono gratuito: 00 800 6 7 8 9 10 11 (algunos operadores pueden cobrar por las llamadas);
— marcando el siguiente número de teléfono: +32 22999696; o
— por correo electrónico: https://europa.eu/european-union/contact_es

Buscar información sobre la Unión Europea

En línea
Puede encontrar información sobre la Unión Europea en todas las lenguas oficiales de la Unión en el sitio web Europa: https://europa.eu/european-union/index_es

Publicaciones de la Unión Europea
Puede descargar o solicitar publicaciones gratuitas y de pago de la Unión Europea en: https://publications.europa.eu/es/publications. Si desea obtener varios ejemplares de las publicaciones gratuitas, póngase en contacto con Europe Direct o su centro de información local (https://europa.eu/european-union/contact_es).

Derecho de la Unión y documentos conexos
Para acceder a la información jurídica de la Unión Europea, incluido todo el Derecho de la Unión desde 1952 en todas las versiones lingüísticas oficiales, puede consultar el sitio web EUR-Lex: https://eur-lex.europa.eu

Datos abiertos de la Unión Europea
El portal de datos abiertos de la Unión Europea (http://data.europa.eu/euodp/es) permite acceder a conjuntos de datos de la Unión. Los datos pueden descargarse y reutilizarse gratuitamente con fines comerciales o no comerciales.