Universidad Zaragoza

Contexto normativo y gestión de riesgos

Grado en Ingeniería en Informática

Curso 2024-2025

Francisco Javier López Pellicer (fjlopez@unizar.es)
Carlos Tellería Orriols (telleria@unizar.es)
Fernando Tricas García (ftricas@unizar.es)
Raquel Trillo Lado (raqueltl@unizar.es)
Dpto. Informática e Ingeniería de Sistemas

Legislación vigente

Penal

- Código Penal (LO 10/1995, de 23 de noviembre)
  Artículos 187, 197-200, 248, 256, 264, 270 y 278

Extrapenal

- LOPD (LO 15/1999, de 13 de diciembre)
- RLOPD (RD 1720/2007, de 21 de diciembre)
- LOPD-GDD (LO 3/2018, de 5 de diciembre)

GDPR
Mayo 2018

- LSSI-CE (LEY 34/2002, de 11 de julio)
- LPI (Real Decreto Legislativo 1/1996, de 12 de abril)
- Real Decreto 1337/1999 Sociedad de la info., de 31 de julio
- Ley 56/2007 de Medidas de Impulso de la Soc. de la Información (28 de diciembre)
- Firma electrónica (Ley 59/2003, de 19 de diciembre)
- Directiva EU 95/46/CE, de 24 de octubre
- ENS (Real Decreto 3/2010, de 8 de enero)

Universidad Zaragoza

Normas principales

Marco legal

CE	• Constitución Española - 1978 (artículo 18)
LOPD	• Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal
RLOPD	• Real Decreto 1720/2007, Reglamento de desarrollo de la Ley Orgánica 15/1999
RGPD	• Reglamento (UE) 2016/679, Reglamento General de Protección de Datos
LOPD-GDD	• Ley Orgánica 3/2018

Universidad Zaragoza

Constitución

Artículo 18 de la Constitución Española

- Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
- Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
- La ley **limitará el uso de la informática** para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Universidad Zaragoza

LOPD. (15/1999)

Artículo 1.

- **Objeto.**
- La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al **tratamiento de los datos personales**, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Universidad Zaragoza
1542

Reglamento General de Protección de Datos (UE) 2016/679 de 27 de abril. RGPD.

- Relativo a la protección delas personas físicas en lo que respecta al **tratamiento de datos personales y a la libre circulación de estos datos** y por el que se derogala Directiva 95/46/CE (Reglamento general de protección dedatos)

Universidad Zaragoza

LOPD y Garantía de los Derechos Digitales

- Ley Orgánica 3/2018, de 5 de diciembre
- Deroga la LOPD (15/1999)
- Objeto:

a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones

b) El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/67 y en esta ley orgánica

Universidad Zaragoza

LOPD y Garantía de los Derechos Digitales

Artículo 1. Objeto de la ley.

La presente ley orgánica tiene por objeto:

a) **Adaptar** el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la **protección de las personas físicas en lo que respecta al tratamiento de sus datos personales** y a la libre circulación de estos datos, y completar sus disposiciones.

El **derecho fundamental de las personas físicas a la protección de datos personales**, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.

b) **Garantizar los derechos digitales** de la ciudadanía

AEPD

Agencia Española de protección de datos

https://www.aepd.es/

Universidad Zaragoza
1542

Vocabulario

Dato	Una información sobre una persona física identificada o identificable.
Fichero	Datos, contenidos en cualquier programa o soporte, organizados para que podamos usarlos y recuperarlos
Tratamiento	Recogida, registro, modificación, consulta, destrucción… de datos personales
Responsable	Quien decide qué datos va a tratar, cómo los recogerá, qué uso piensa darles y cómo los tratará
Encargado	Quien trata datos personales por cuenta del responsable del tratamiento

Universidad Zaragoza

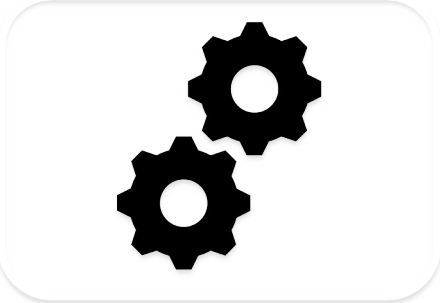
Ayudas protección de datos en AEPD

Derechos del ciudadano

Guía del responsable

Reglamento europeo

Guías



Herramientas

https://www.aepd.es/guias-y-herramientas/guias/decalogo-de-recursos-de-ayuda

Universidad Zaragoza
1542

Sanciones

Que tu hijo menor cree un Instagram con la foto de otro niño cuesta dinero en España: multa de 10.000€ al padre, por la AEPD

El perfil de Instagram con la foto de otro niño estuvo abierto durante dos meses y tenía también un vídeo sexual. El padre alegó que era una broma entre niños

4 comentarios

https://www.genbeta.com/actualidad/padre-tendra-que-pagar-multa-10-000-euros-espana-porque-su-hijo-menor-uso-foto-otro-nino-instagram

Universidad Zaragoza
1542

Principales derechos del ciudadano

- Derecho de información
- Derecho de **A**cceso
- Derecho de **R**ectificación
- Derecho de **C**ancelación
- Derecho de **O**posición

Universidad Zaragoza
1542

Principales derechos del ciudadano

Derecho de acceso

El derecho de acceso se puede ejercitar para conocer si el responsable está tratando o no los datos de carácter personal del solicitante y, en el caso de que se esté realizando dicho tratamiento, obtener la siguiente información:

- Una copia de los datos personales que son objeto del tratamiento
- Los fines del tratamiento
- Las categorías de datos personales que se traten
- Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular, los destinatarios en países terceros u organizaciones internacionales
- El plazo previsto de conservación de los datos personales, o los criterios utilizados para determinar este plazo
- La existencia del derecho del interesado a solicitar al responsable: la rectificación o supresión de sus datos personales, la limitación del tratamiento de sus datos personales u oponerse a ese tratamiento
- El derecho a presentar la Agencia Española de Protección de Datos
- En el caso de que los datos personales no se hayan obtenido directamente del interesado, la información disponible sobre su origen
- En su caso, la existencia de decisiones automatizadas, incluida la elaboración de perfiles, y al menos en tales casos, información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de ese tratamiento para el interesado
- En su caso, si se transfieren datos personales a un tercer país o a una organización internacional, la información sobre las garantías adecuadas en las que se realizan las transferencias

Universidad Zaragoza
1542

Principales derechos del ciudadano

Derecho de rectificación

- El derecho de rectificación se puede ejercitar si los datos personales incluidos en una actividad de tratamiento son inexactos, y deben ser rectificados sin dilación indebida del responsable.
- Teniendo en cuenta los fines del tratamiento, mediante este derecho se puede solicitar que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Universidad Zaragoza
1542

Principales derechos del ciudadano

Derecho de oposición

El derecho de oposición se puede ejercitar para oponerse a que el responsable realice un tratamiento de los datos personales en los siguientes supuestos:

Cuando sean objeto de tratamiento basado en una misión de interés público o en el interés legítimo, incluido la elaboración de perfiles:

- El responsable dejará de tratar los datos salvo que acredite motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones

Cuando el tratamiento tenga como finalidad la mercadotecnia directa, incluida también la elaboración de perfiles anteriormente citada:

- Ejercitado este derecho para esta finalidad, los datos personales dejarán de ser tratados para dichos fines

Universidad Zaragoza
1542

Principales derechos del ciudadano

Derecho de supresión ("al olvido")

El derecho al olvido se puede ejercitar cuando concurra alguna de las siguientes circunstancias:

- Si los datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo
- Si el tratamiento de tus datos personales se ha basado en el consentimiento prestó al responsable, y se retira el mismo, siempre que el citado tratamiento no se base en otra causa que lo legitime
- Si se ha opuesto al tratamiento de tus datos personales al ejercitar el derecho de oposición en las siguientes circunstancias
    - El tratamiento del responsable se fundamentaba en el interés legítimo o en el cumplimiento de una misión de interés público, y no han prevalecido otros motivos para legitimar el tratamiento de tus datos
    - A que los datos personales sean objeto de mercadotecnia directa, incluyendo la elaboración perfiles relacionada con la citada mercadotecnia
- Si los datos personales han sido tratados ilícitamente
- Si los datos personales deben suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento
- Si los datos personales se han obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1 (condiciones aplicables al tratamiento de datos de los menores en relación con los servicios de la sociedad de la información).

Universidad Zaragoza
1542

Principales obligaciones del profesional

- Elaboración de un registro.
- Calidad de los datos
- Deber de guardar secreto
- Deber de información
- Atención de los derechos de los ciudadanos

Universidad Zaragoza

Organizaciones:
Principio de responsabilidad proactiva

Análisis de

Qué datos tratar, Para qué, Cómo

Desarrollo explícito de

Cómo aplicar RGPD

Capacitando para

Demostrar que se cumple el RGPD

Universidad Zaragoza
1542

Consentimiento inequívoco

El consentimiento inequívoco es aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa.

A diferencia del Reglamento de Desarrollo de la LOPD, no se admiten formas de consentimiento tácito o por omisión, ya que se basan en la inacción

Universidad Zaragoza
1542

Transparencia

La información a los interesados deberá proporcionarse de forma

concisa

transparente

inteligible

de fácil acceso

con un lenguaje sencillo

Universidad Zaragoza

Resumen derechos RGPD

Derechos **ARCO**

Derecho al **olvido** (como consecuencia de los derechos de cancelación y oposición)

Derecho a la **portabilidad**

Derecho de acceso avanzado: los datos se reciben en un formato estructurado, de uso común y lectura mecánica

Consecuencia: los datos personales del interesado se transmiten directamente de un responsable a otro

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Universidad Zaragoza
1542

Resumen derechos RGPD

Derecho a la portabilidad

El derecho a la portabilidad se puede ejercer para recibir los datos personales de un responsable en un formato estructurado, de uso común, de lectura mecánica e interoperable, que permita transmitirlos a otro responsable de tratamiento, siempre que el tratamiento se legitime en base al consentimiento o en el marco de la ejecución de un contrato.

Universidad Zaragoza
1542

Resumen derechos RGPD

Derecho a no ser objeto de decisiones individuales automatizadas

Este derecho garantiza a los titulares de datos personales que no sean objeto de una decisión basada únicamente en el tratamiento de datos, incluida la elaboración de perfiles, que pueda produzca efectos jurídicos.

Se considera elaboración de perfiles, cualquier forma de tratamiento de los datos personales que evalúe aspectos personales que permita, en particular, analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento.

https://www.aepd.es/derechos-y-deberes/conoce-tus-derechos

Universidad Zaragoza
1542

Delegado de protección de datos

Nueva figura de RGPD

Obligatorio en 3 supuestos:

- Autoridades y organismos públicos
- Cuando responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala
- Cuando responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles (categorías especiales / relacionados con delitos)

Universidad Zaragoza

Delegado de protección de datos

Ejemplos

Colegios profesionales

Centros docentes de todos los niveles, desde escuelas infantiles hasta la universidad

Empresas de telecomunicaciones y otros prestadores de servicios de la sociedad de la información (cuando elaboren a gran escala perfiles de los usuarios)

Entidades bancarias y compañías de seguros
Compañías de energía, electricidad y gas

Responsables de ficheros de morosos

Responsables de los ficheros regulados por la ley de prevención del blanqueo de capitales (entidades de crédito, compañías de seguros, agencias inmobiliarias, casinos, joyeros…)

Universidad Zaragoza
1542

Delegado de protección de datos

Agencias de publicidad (cuando elaboren perfiles de los usuarios)

Centros sanitarios de cualquier tamaño y especialidad (excepto consultas individuales)

Entidades que realicen informes comerciales de personas físicas

Operadores de juego online

Empresas de seguridad privada

Federaciones deportivas (cuando traten con menores de edad)

Universidad Zaragoza
1542

Responsable del tratamiento

Persona física o jurídica, o bien una autoridad pública

La responsabilidad última sobre el tratamiento es del responsable

Los responsables habrán de elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento

Universidad Zaragoza
1542

Obligaciones propias del *encargado* del tratamiento

Mantener un registro de actividades de tratamiento

Determinar las medidas de seguridad aplicables a los tratamientos que realizan

Designar (junto a los responsables) a un Delegado de Protección de Datos en los casos previstos por el RGPD

Universidad Zaragoza
1542

Responsable - Encargado

Sólo habrá encargado si lo decide el responsable

Las relaciones entre el responsable y el encargado deben formalizarse en un contrato o en un acto jurídico que vincule al encargado respecto al responsable

Se regula de forma minuciosa el contenido mínimo de los contratos de encargo

Universidad Zaragoza
1542

Análisis de riesgos

Todos los responsables deberán realizar una **valoración del riesgo** de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo

Universidad Zaragoza
1542

Análisis de riesgos

El enfoque de riesgos en protección de datos tiene al menos dos vertientes:

- La orientada a determinar las medidas de seguridad **técnicas y organizativas** para proteger los datos personales
- Los riesgos para los **derechos y libertades** de las personas

Universidad Zaragoza
1542

Análisis de riesgos

Se materializa en:

- La protección de datos desde el diseño
- La protección de datos por defecto
- Las evaluaciones de impacto.

Universidad Zaragoza
1542

Análisis de riesgos

FASES

COMUNICACIÓN: involucrar a toda la organización, identificar riesgos y probabilidades de que los mismos se materialicen, establecer prioridades y objetivos, concienciación y formación del personal.

CONTEXTO: definir el marco en el que se desarrolla la política de análisis de riesgos teniendo en cuenta normativas aplicables, riesgos aceptables y el mapa de elementos implicados en los tratamientos de datos personales (activos).

IDENTIFICAR RIESGOS: elaboración del mapa de riesgos de la organización, cuantificar posibles daños.

ANALIZAR Y EVALUAR EL RIESGO: mediante escalas cuantitativas o cualitativas se establecen valores objetivos para cada riesgo.

GESTIONAR EL RIESGO: determinar para cada riesgo las salvaguardas aplicables teniendo en cuenta la relación costo-beneficio que pueda existir en cada caso.

SEGUIMIENTO DEL RIESGO:auditorías, informes, incorporación de activos, en general cualquier cambio que implique una modificación del riesgo y sus salvaguardas correspondientes.

https://www.aepd.es/prensa-y-comunicacion/blog/el-enfoque-de-riesgos-en-el-reglamento

Universidad Zaragoza
1542

Infracciones y sanciones

Muy graves: las que supongan un incumplimiento sustancial del tratamiento y tengan que ver con:

- Uso de los datos para una finalidad diferente a la pactada.
- Omisión del deber de correcta información al afectado.
- Exigencia de un pago para poder acceder a los datos propios almacenados.
- Transferencia internacional de información sin garantías.

Hasta 20m€ o 4% facturación

Plazo de prescripción: 3 años

Graves: vulneración sustancial del tratamiento y tengan que ver con:

Hasta 10m€ o 2% facturación

- Datos de un menor recabados sin consentimiento.
- Falta de adopción de medidas técnicas y organizativas necesarias para la efectiva protección de datos.
- Incumplimiento de nombrar responsable o encargado de tratamiento de datos.

Plazo de prescripción: 2 años.

Leves: Las restantes no contempladas en los grupos anteriores.

- No transparencia de la información.
- Incumplimiento de no informar al afectado cuando lo haya solicitado.
- Incumplimiento por parte del encargado de sus obligaciones.

Plazo de prescripción: 1 año.

Universidad Zaragoza

¿Sólo nosotros?

Year	Industry & Government Reactions	Industry or Criteria
1995	European Privacy Law	Protects the privacy of individuals when their data is processed or transmitted
1996	HIPAA – Health Insurance Portability and Accountability Act	Healthcare
1996	Economic Espionage Act	Makes the theft or misappropriation of trade secrets involving commercial information, not classified or national defense information, a federal crime
1999	GLBA - Gramm-Leach-Bliley Act	Financial Services
2002	FISMA - Federal Information Security Management Act	US Federal Government
2002	SOX - Sarbanes-Oxley	Public Companies
2003	CA SB 1386 - California Senate Bill 1386 (40+ states have followed suit)	Requiring organizations that maintain personal information about individuals to inform those individuals if the security of their information is compromised
2004	Basel II	Financial Services
2006	PCI DSS – Payment Card Industry Data Security Standard	Companies processing credit card data
2006	NERC CIPS – North American Electric Reliability Corporation Critical Infrastructure Protection Standards	Electric Power
2008	Red Flags Rule	Financial Services
2009	HITECH - Health Information Technology for Economic and Clinical Health Act	Healthcare

Universidad Zaragoza

“There are two problems to solve. The first is information asymmetry: Buyers can’t adequately judge the security of software products or company practices. The second is a perverse incentive structure: The market encourages companies to make decisions in their private interest, even if that imperils the broader interests of society. Together these two problems result in companies that save money by taking on greater risk and then pass off that risk to the rest of us, as individuals and as a nation.

The only way to force companies to provide safety and security features for customers and users is with government intervention. Companies need to pay the true costs of their insecurities, through a combination of laws, regulations and legal liability. Governments routinely legislate safety — pollution standards, automobile seatbelts, lead-free gasoline, food service regulations. We need to do the same with cybersecurity: The federal government should set minimum security standards for software and software development.”

Bruce Schneier. Why Was SolarWinds So Vulnerable to a Hack? It’s the economy, stupid. The New York Times. 23 de febrero de 2021

Universidad Zaragoza
1542

THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

FEBRUARY 2003

THE WHITE HOUSE
WASHINGTON

My Fellow Americans:

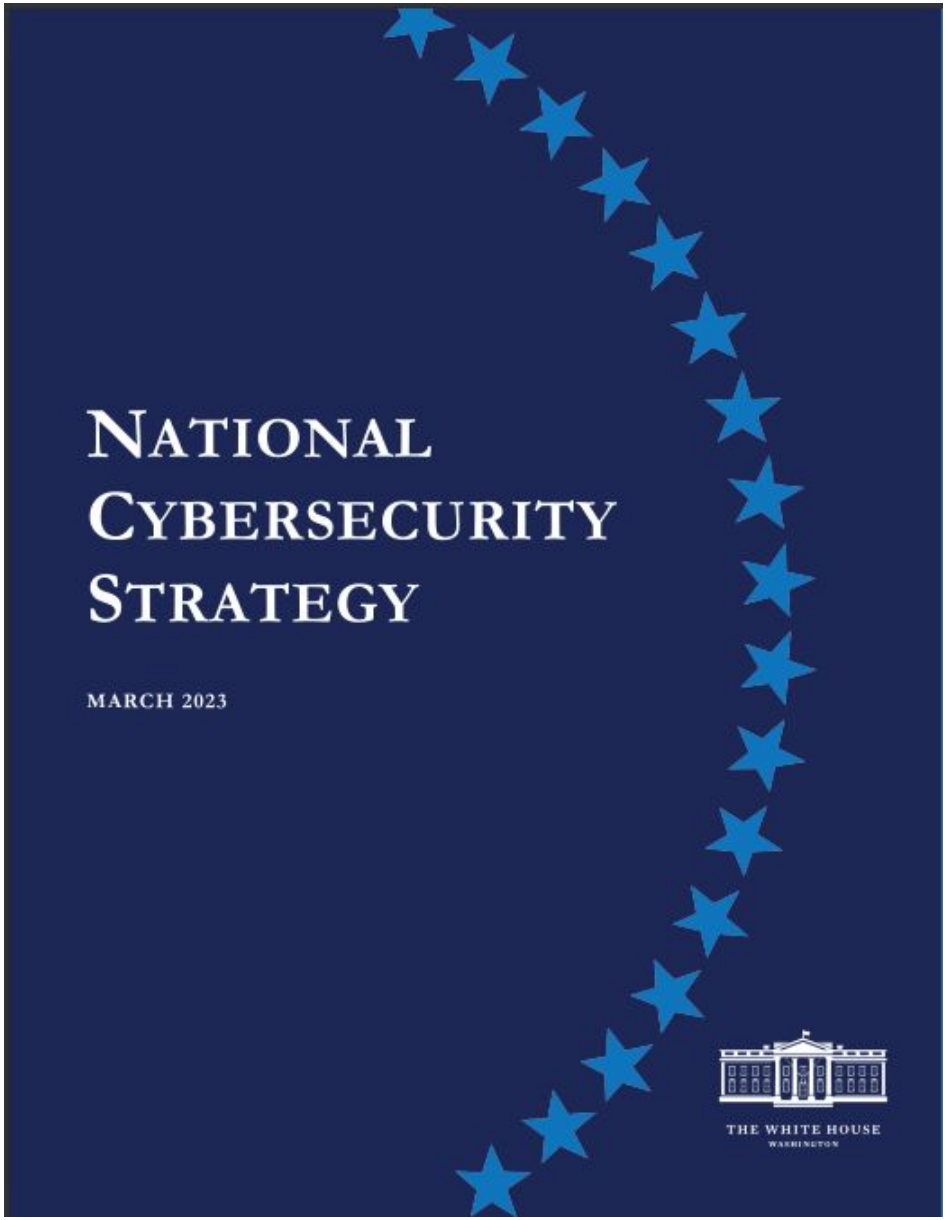
The way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependent network of information technology infrastructures called cyberspace. The *National Strategy to Secure Cyberspace* provides a framework for protecting this infrastructure that is essential to our economy, security, and way of life.

In the past few years, threats in cyberspace have risen dramatically. The policy of the United States is to protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States. We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation's critical infrastructures and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible.

Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people. To engage Americans in securing cyberspace, a draft version of this strategy was released for public comment, and ten town hall meetings were held around the Nation to gather input on the development of a national strategy. Thousands of people and numerous organizations participated in these town hall meetings and responded with comments. I thank them all for their continuing participation.

The cornerstone of America's cyberspace security strategy is and will remain a public-private partnership. The federal government invites the creation of, and participation in, public-private partnerships to implement this strategy. Only by acting together can we build a more secure future in cyberspace.

Universidad Zaragoza
1542



THE WHITE HOUSE
WASHINGTON

March 1, 2023

Digital technologies today touch nearly every aspect of American life. The openness and connection enabled by access to the Internet are game-changers for communities everywhere, as we have all experienced throughout the COVID-19 pandemic. That's why, thanks to the Bipartisan Infrastructure Law, my Administration is investing $65 billion to make sure every American has access to reliable, high-speed Internet. And when we pick up our smart phones to keep in touch with loved ones, log on to social media to share our ideas with one another, or connect to the Internet to run a business or take care of any of our basic needs, we need to be able to trust that the underlying digital ecosystem is safe, reliable, and secure. This National Cybersecurity Strategy details the comprehensive approach my Administration is taking to better secure cyberspace and ensure the United States is in the strongest possible position to realize all the benefits and potential of our digital future.

Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense. From the very beginning of my Administration, we have moved decisively to strengthen cybersecurity. I appointed senior cybersecurity officials at the White House and issued an Executive Order on Improving the Nation's Cybersecurity. Working in close cooperation with the private sector, my Administration has taken steps to protect the American people from hackers, hold bad actors and cybercriminals accountable, and defend against the increasingly malicious cyber campaigns targeting our security and privacy. And we've worked with our allies and partners around the world to improve our capacity to collectively defend against and respond to cyber threats from authoritarian states that go against our national interests.

This strategy recognizes that robust collaboration, particularly between the public and private sectors, is essential to securing cyberspace. It also takes on the systemic challenge that too much of the responsibility for cybersecurity has fallen on individual users and small organizations. By working in partnership with industry; civil society; and State, local, Tribal, and territorial governments, we will rebalance the responsibility for cybersecurity to be more effective and more equitable. We will realign incentives to favor long-term investments in security, resilience, and promising new technologies. We will collaborate with our allies and partners to strengthen norms of responsible state behavior, hold countries accountable for irresponsible behavior in cyberspace, and disrupt the networks of criminals behind dangerous cyberattacks around the globe. And we will work with the Congress to provide the resources and tools necessary to ensure effective cybersecurity practices are implemented across our most critical infrastructure.

As I have often said, our world is at an inflection point. That includes our digital world. The steps we take and choices we make today will determine the direction of our world for decades

Universidad Zaragoza
1542

Esquema Nacional de Seguridad

Universidad Zaragoza
1542

Esquema Nacional de Seguridad

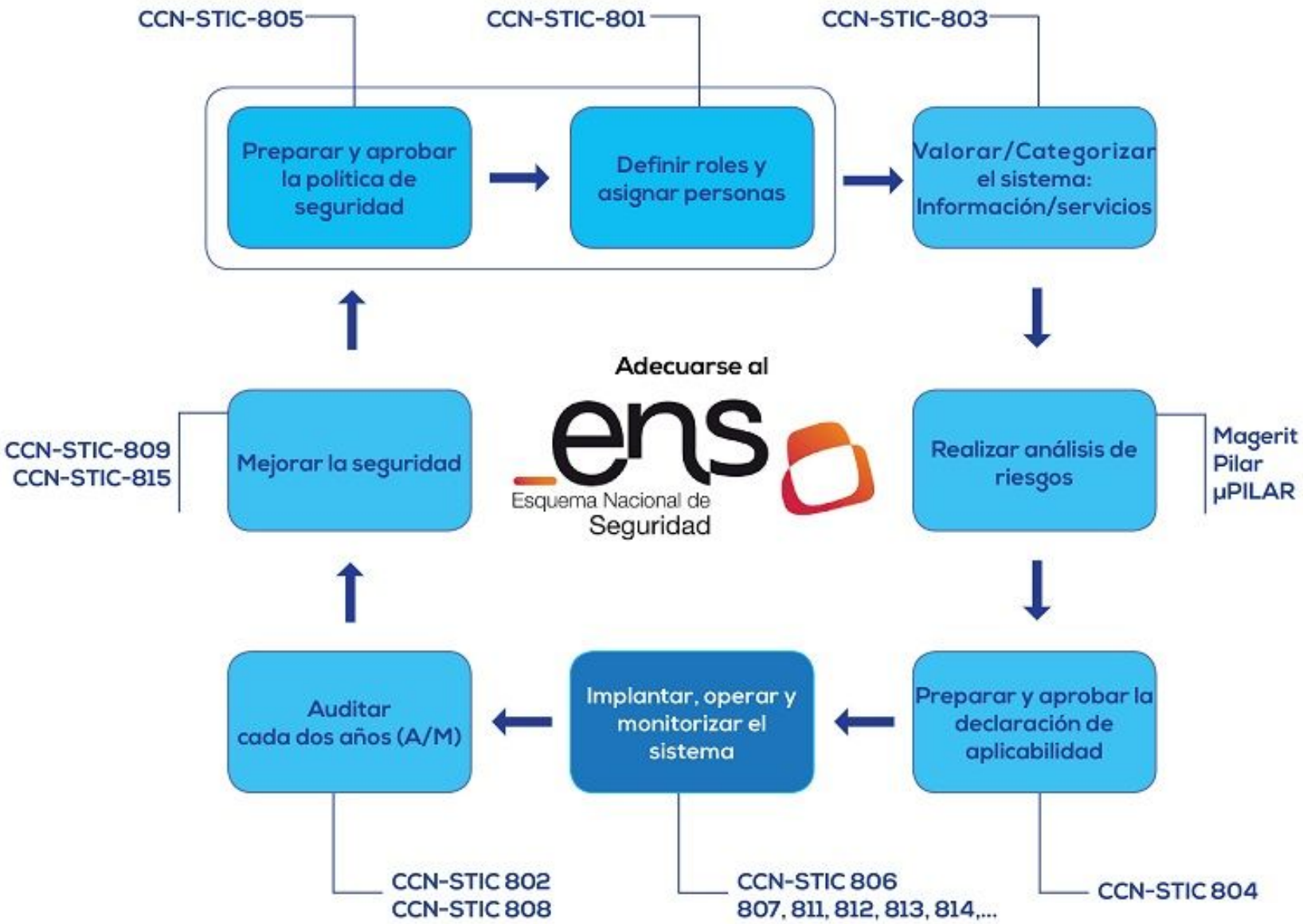
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS) establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.
- Actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración,
- Sustituido por el Real Decreto 311/2022

Universidad Zaragoza

Esquema Nacional de Seguridad Principios.

a. Seguridad como proceso integral. “único proceso para todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información”
b. Gestión de la seguridad basada en los riesgos.
c. Prevención, detección, respuesta y conservación.
d. Existencia de líneas de defensa.
e. Vigilancia continua.
f. Re-evaluación periódica.
g. Diferenciación de responsabilidades.

“Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos ”


CCN-STIC-805
CCN-STIC-801
CCN-STIC-803
Preparar y aprobar la política de seguridad
Definir roles y asignar personas
Valorar/Categorizar el sistema: Información/servicios
Adecuarse al
ens
Esquema Nacional de Seguridad
Realizar análisis de riesgos
Magerit
Pilar
µPILAR
Preparar y aprobar la declaración de aplicabilidad
Implantar, operar y monitorizar el sistema
Auditar cada dos años (A/M)
Mejorar la seguridad
CCN-STIC-809
CCN-STIC-815
CCN-STIC 802
CCN-STIC 808
CCN-STIC 806
807, 811, 812, 813, 814,...
CCN-STIC 804

Normas principales

Marco legal

Directiva NIS2

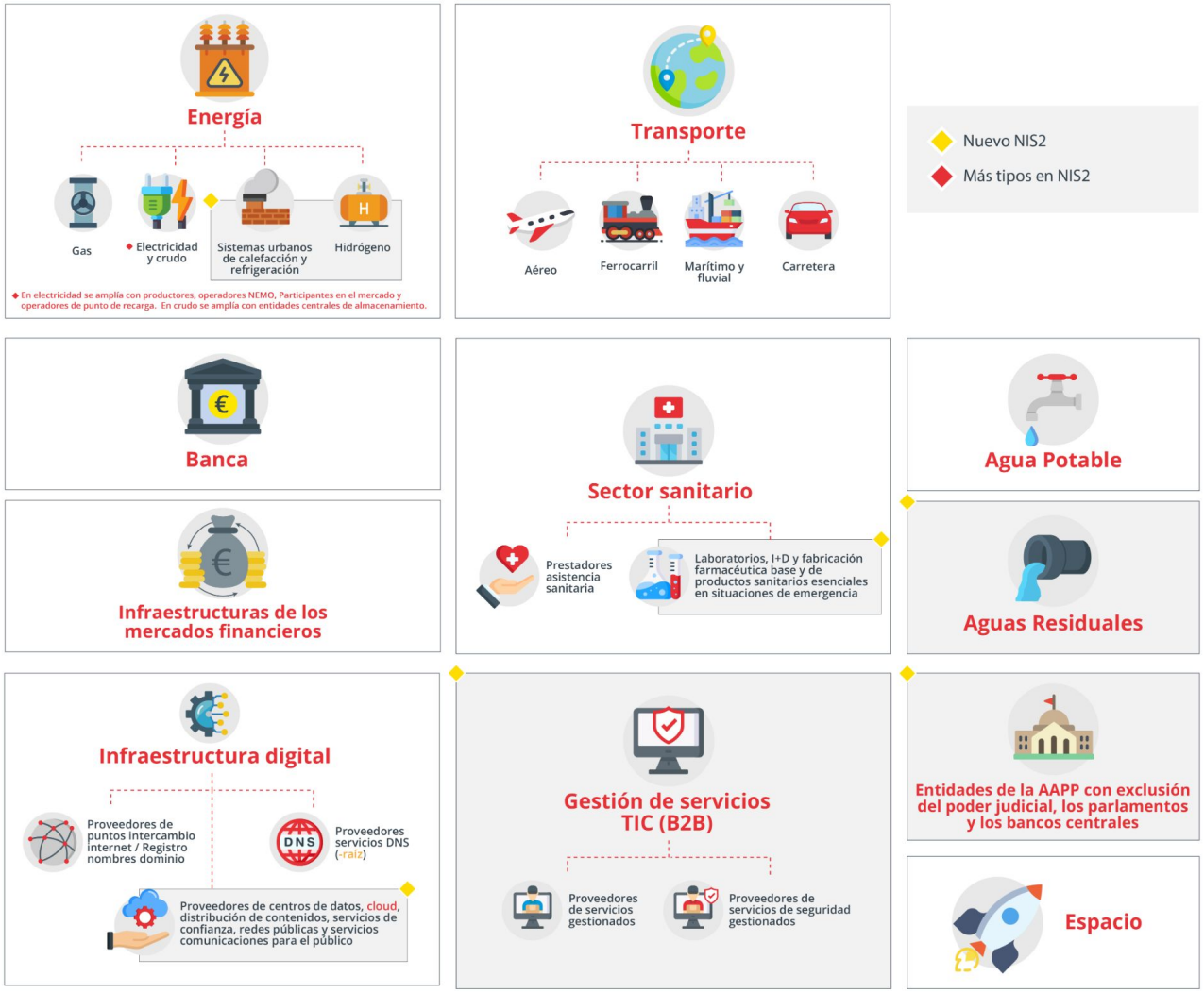
Todavía no hay trasposición española.

https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

Universidad Zaragoza
1542

Sectores en el ámbito de NIS2

Anexo I: Sectores de alta criticidad



Universidad Zaragoza
1542

Normas principales

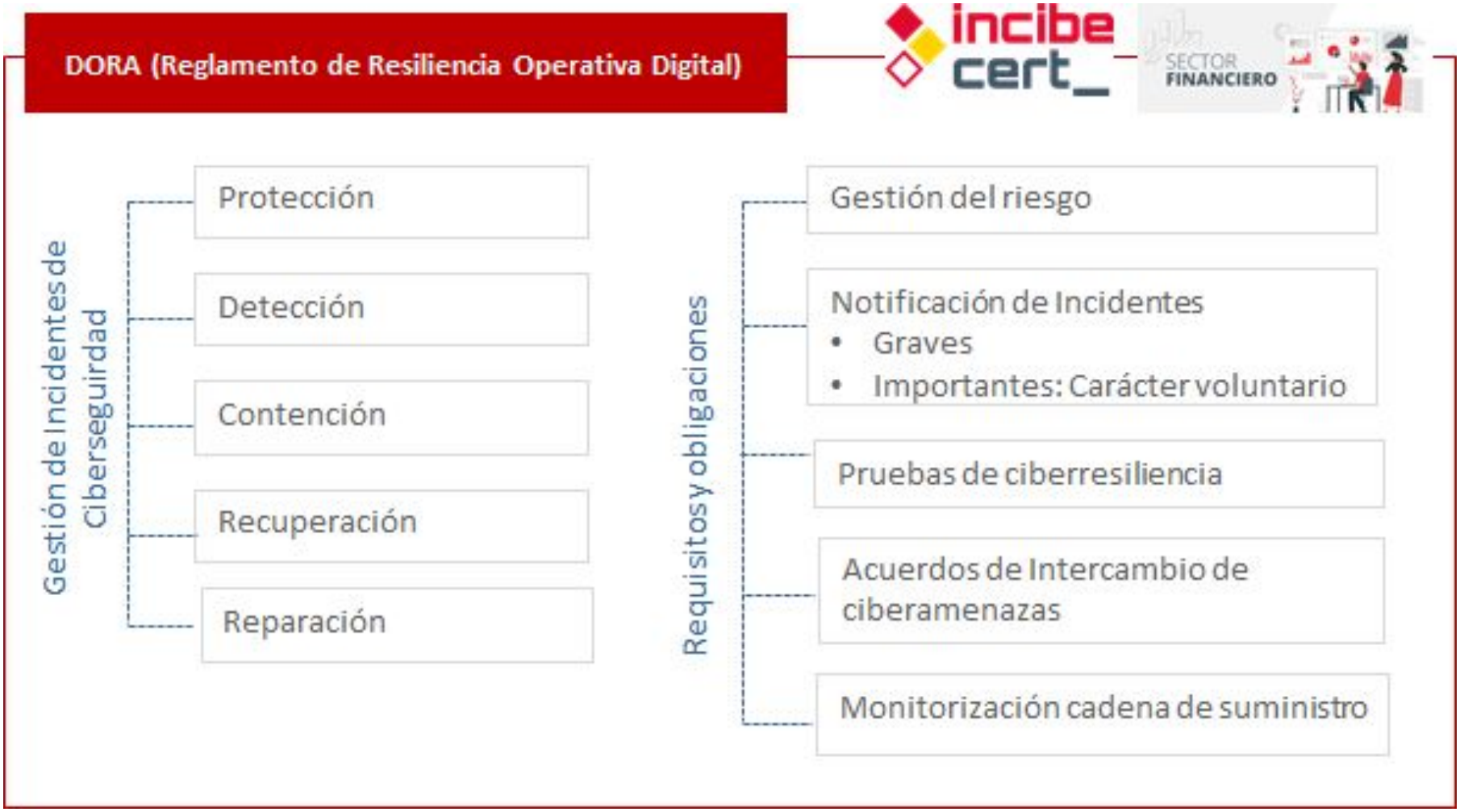
Sectores en el ámbito de NIS2

Anexo 2: Otros sectores críticos

https://www.incibe.es/incibe-cert/sectores-estrategicos/FAQNIS2

Universidad Zaragoza

DORA (Digital Operational Resilience Act)



https://www.incibe.es/empresas/blog/que-es-el-reglamento-dora

Universidad Zaragoza
1542

DORA (Digital Operational Resilience Act)

Requisitos de DORA para Entidades Financieras

incibe cert_

SECTOR FINANCIERO

PASO 1 → PASO 2 → PASO 3 → PASO 4

PASO 1	PASO 2	PASO 3	PASO 4
Gestión y gobernanza del riesgo de TIC	Notificación de incidentes	Pruebas de resiliencia, e intercambio de amenazas	Gestión de riesgos de terceros

PASO 1

Desarrollo de marcos integrales de gestión del riesgo
Identificación y clasificación de activos críticos
Evaluaciones continuas de riesgos
Establecimiento de medidas de ciberseguridad adecuadas
Responsabilidad del órgano de dirección

PASO 2

Establecimiento de sistemas de monitoreo, gestión y registro de incidentes
Obligación de informar a autoridades competentes, clientes y socios
Presentación de informes inicial, intermedio y final

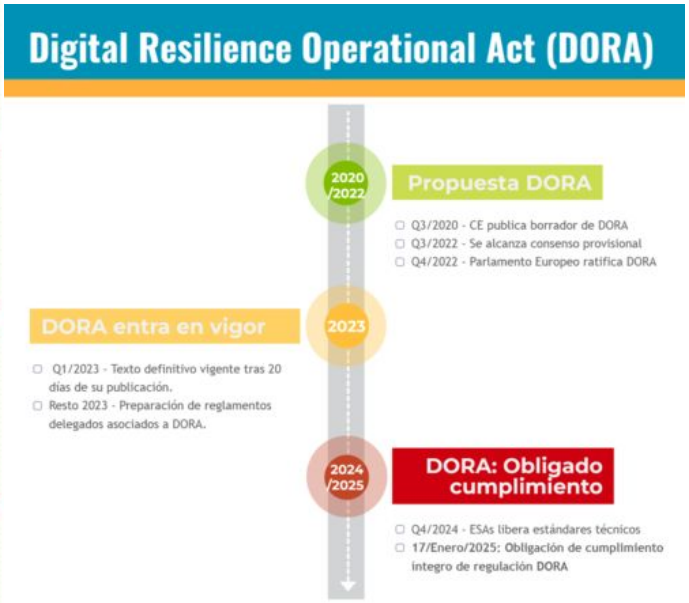
PASO 3

Pruebas regulares de sistemas de TIC
Evaluaciones de vulnerabilidades y pruebas basadas en escenarios
Pruebas de penetración con amenazas específicas
Establecimiento de acuerdos de intercambio de información e inteligencia

PASO 4

Papel activo en la gestión del riesgo de terceros de TIC
- Establecimiento de acuerdos contractuales específicos
- Mapeo de dependencias de la cadena de suministro
- Supervisión directa de proveedores de servicios críticos
- Cumplimiento de requisitos de DORA por parte de proveedores

Entidades financieras



https://www.incibe.es/empresas/blog/que-es-el-reglamento-dora

Universidad Zaragoza
1542

Referencias y bibliografía

INCIBE, Insituto Nacional de CIBERseguridad, http://www.incibe.es

Agencia Española de Protección de Datos: http://www.aepd.es

Universidad Zaragoza
1542

Introducción a la auditoría de Sistemas de Información y Seguridad MAGERIT

Grado en Ingeniería en Informática

Curso 2024-2025

Francisco Javier López Pellicer (fjlopez@unizar.es)
Carlos Tellería Orriols (telleria@unizar.es)
Fernando Tricas García (ftricas@unizar.es)
Raquel Trillo Lado (raqueltl@unizar.es)
Dpto. Informática e Ingeniería de Sistemas

Universidad Zaragoza
1542

Introducción a MAGERIT

Metodología de Análisis y Gestión de Riesgos orientada a Sistemas de información y Comunicación

Consejo Superior de Administración Electrónica de España
Utilizada en el **ámbito público y privado**

Objetivos:

Concienciar de la existencia de riesgos y de la necesidad de gestionarlos

Ofrecer un método sistemático (**modelo**) para analizar los riesgos y gestionarlos

Ayudar a **descubrir riesgos** y **planificar** su tratamiento

Facilitadora para auditorías, certificaciones, concursos, ...

Universidad Zaragoza
1542

Introducción a MAGERIT

Garantizar:

Confidencialidad: sólo accesos autorizados

Integridad: información no alterada/transformada sin autorización

Disponibilidad: accesible en el momento oportuno

Autenticidad: se puede identificar quién la genera

Trazabilidad: qué y cuándo se genera/modifica/borra la información

Durante el ciclo de vida de los datos (en el sistema de información):

En la entrada de datos Su almacenamiento

Procesado

Transmisión

Uso

Destrucción

Universidad Zaragoza
1542

Introducción a MAGERIT

La seguridad total no es viable, siempre existe algún riesgo

Se trata de analizar los riesgos y tomar las medidas oportunas para generar confianza y asumir/aceptar un **cierto nivel de riesgo**

Tratamiento del riesgo:

Evitar las circunstancias que lo provocan

Reducir la probabilidad de que ocurra

Compartirlo con otra organización (externalizándolo)

Aceptar que puede ocurrir y establecer los planes de contingencia y recuperación (Acotar sus consecuencias)

Universidad Zaragoza

Introducción a MAGERIT

MAGERIT nos permite analizar y gestionar de forma metódica, sistemática, objetiva y contrastable los riesgos

Tres libros de referencia:

- Método
- Catálogo
- Guía de técnicas

Se intenta eliminar la arbitrariedad del analista

Universidad Zaragoza
1542

Introducción a MAGERIT

Objetivos

Directos

Concienciar a los responsables de las organizaciones de información de la **existencia de riesgos** y la necesidad de gestionarlos

Ofrecer un **método sistemático** para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos

Preparar a la organización para procesos de **evaluación**, **auditoría**, **certificación** o **acreditación**, según corresponda en cada caso

Universidad Zaragoza
1542

Introducción a MAGERIT

Terminología básica (Libro I – Magerit)

Riesgo

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización

Análisis de riesgos

Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización

Tratamiento de los riesgos

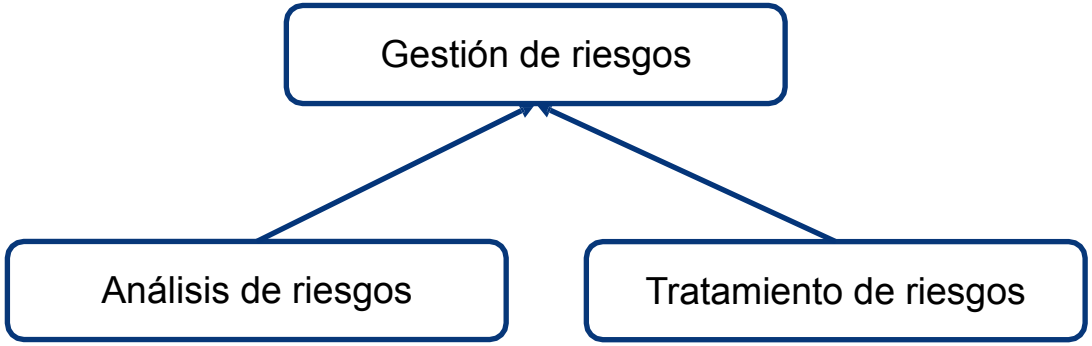
Proceso destinado a modificar el riesgo y reducirlo a un mínimo razonable

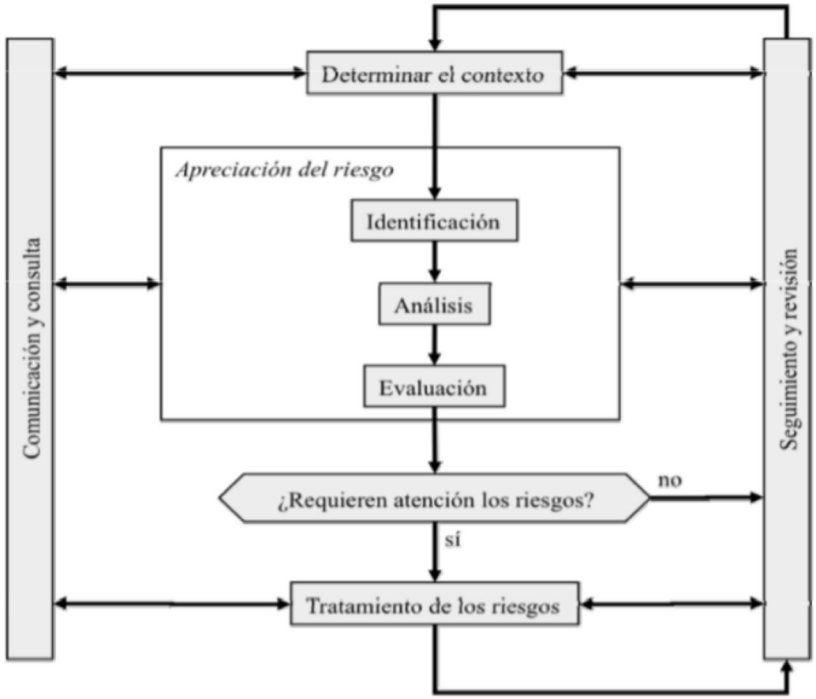
Universidad Zaragoza
1542

Introducción a MAGERIT

Terminología básica

Gestión de riesgos





Universidad Zaragoza
1542

Introducción a MAGERIT

Terminología básica

El análisis de riesgos considera los siguientes elementos

Activos: son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la **misión de la organización**

Esenciales: **información** y **servicios**
Secundarios: datos, servicios auxiliares, aplicaciones informáticas, equipos informáticos, equipamiento auxiliar, redes de comunicaciones, instalaciones y personas

Amenazas: eventos que pueden ocurrir a los activos y que pueden causar un perjuicio a la organización

Salvaguardas: medidas de protección desplegadas para reducir el potencial daño que producen las amenazas

Universidad Zaragoza
1542

Introducción a MAGERIT

Principales pasos en el análisis de MAGERIT

Paso 1. Determinar los **activos** relevantes para la entidad (su **valor** e **interrelación** en el sentido del **coste** que supondría su deterioro). Estudiar la **dependencia** entre activos

Grafos de dependencia: si una amenaza afecta al activo inferior afectará también al activo superior

Dependencias

Propagación del daño (si amenaza se materializa)

Valoración cualitativa o cuantitativa

Valor de la interrupción de un servicio

Dimensiones de los activos: confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad

Universidad Zaragoza
1542

Introducción a MAGERIT

Principales pasos en el análisis de MAGERIT

Paso 2. Determinar las **amenazas** a las que están expuestos esos activos y su impacto en caso de materializarse

Identificación: de origen natural, del entorno, defectos de las aplicaciones, causadas por personas de forma accidental y causadas por personas de forma deliberada

Valoración: si una amenaza afecta a un activo, cómo lo hace:

Degradación: cómo de perjudicado resultaría el activo (totalmente degradado, degradado en una pequeña fracción, ...)

Impacto en la organización:

Valor del activo * Degradación

Probabilidad: de que se materialice la amenaza (baja, alta, muy alta, ...)

Riesgo en la organización:

Impacto * Probabilidad

Universidad Zaragoza
1542

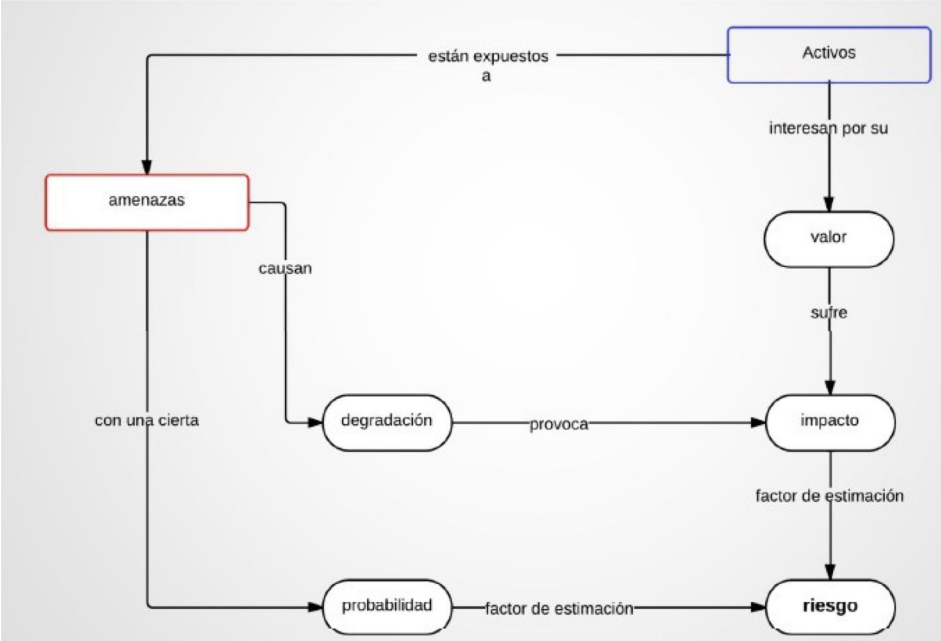
Introducción a MAGERIT

Principales pasos en el análisis de MAGERIT

Paso 2 (cont.). Estimar el **impacto** (daño sobre el activo derivado de la materialización de la amenaza) y el **riesgo** (impacto ponderado por la probabilidad de que se materialice la amenaza)

Impacto acumulado/repercutido (sobre un activo)

Agregación de valores de impacto

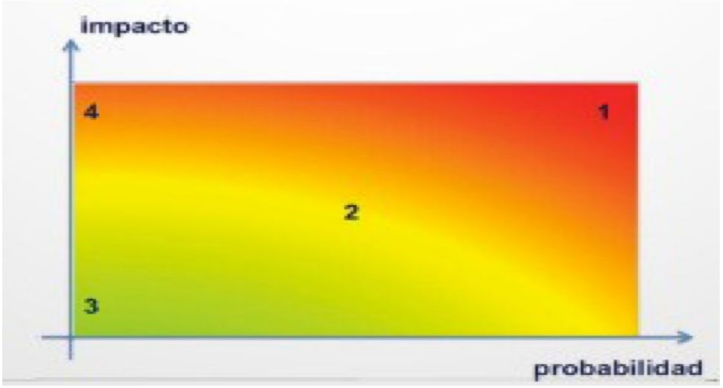


Universidad Zaragoza
1542

Introducción a MAGERIT

Principales pasos en el análisis de MAGERIT

Paso 2 (cont.). Determinar el **riesgo potencial** para cada par <activo, amenaza>. Depende del **impacto** y de la **probabilidad** de materialización de la amenaza



Agregación de riesgos

Universidad Zaragoza
1542

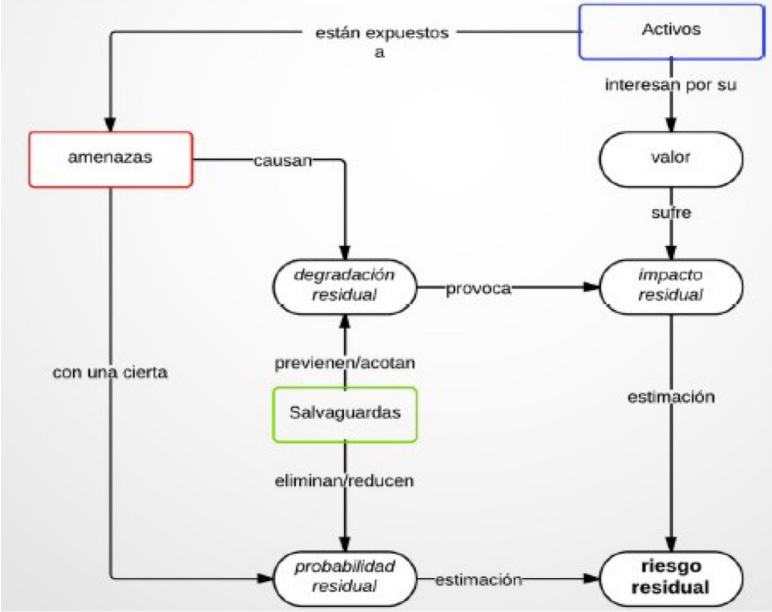
Introducción a MAGERIT

Principales pasos en el análisis MAGERIT

Paso 3. Identificar las medidas de **salvaguarda** (medida que reduce el riesgo) dispuestas y cómo de eficaces son (**impacto** y **riesgo residual**). Pueden:

Reducir la probabilidad de que la amenazas se materialicen

Limitar el daño causado si se se materializan

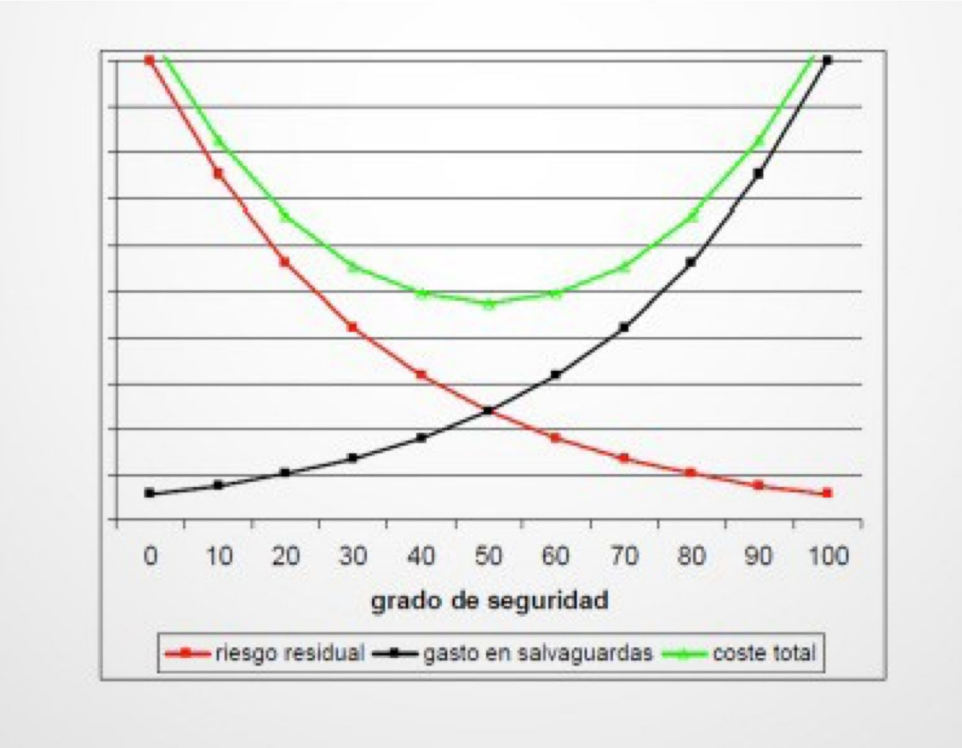


Universidad Zaragoza

Introducción a MAGERIT

Principales pasos en el análisis MAGERIT

Paso 3 (cont.). A la hora de plantear una salvaguarda y decidir si implantarla o no es necesario hacer un estudio cuantitativo entre el coste y el beneficio



Universidad Zaragoza
1542

Introducción a MAGERIT

Principales pasos en el análisis MAGERIT

Paso 4. Determinar el **impacto residual** por cada activo y amenaza que le pueda afectar

Reevaluación del impacto teniendo en cuenta la eficacia de las salvaguardas (sólo debería cambiar la magnitud de la degradación)

Paso 5. Determinar el **riesgo residual** por cada activo y amenaza que le pueda afectar

Reevaluación del riesgo teniendo en cuenta el impacto residual y la probabilidad residual

Universidad Zaragoza
1542

Introducción a MAGERIT

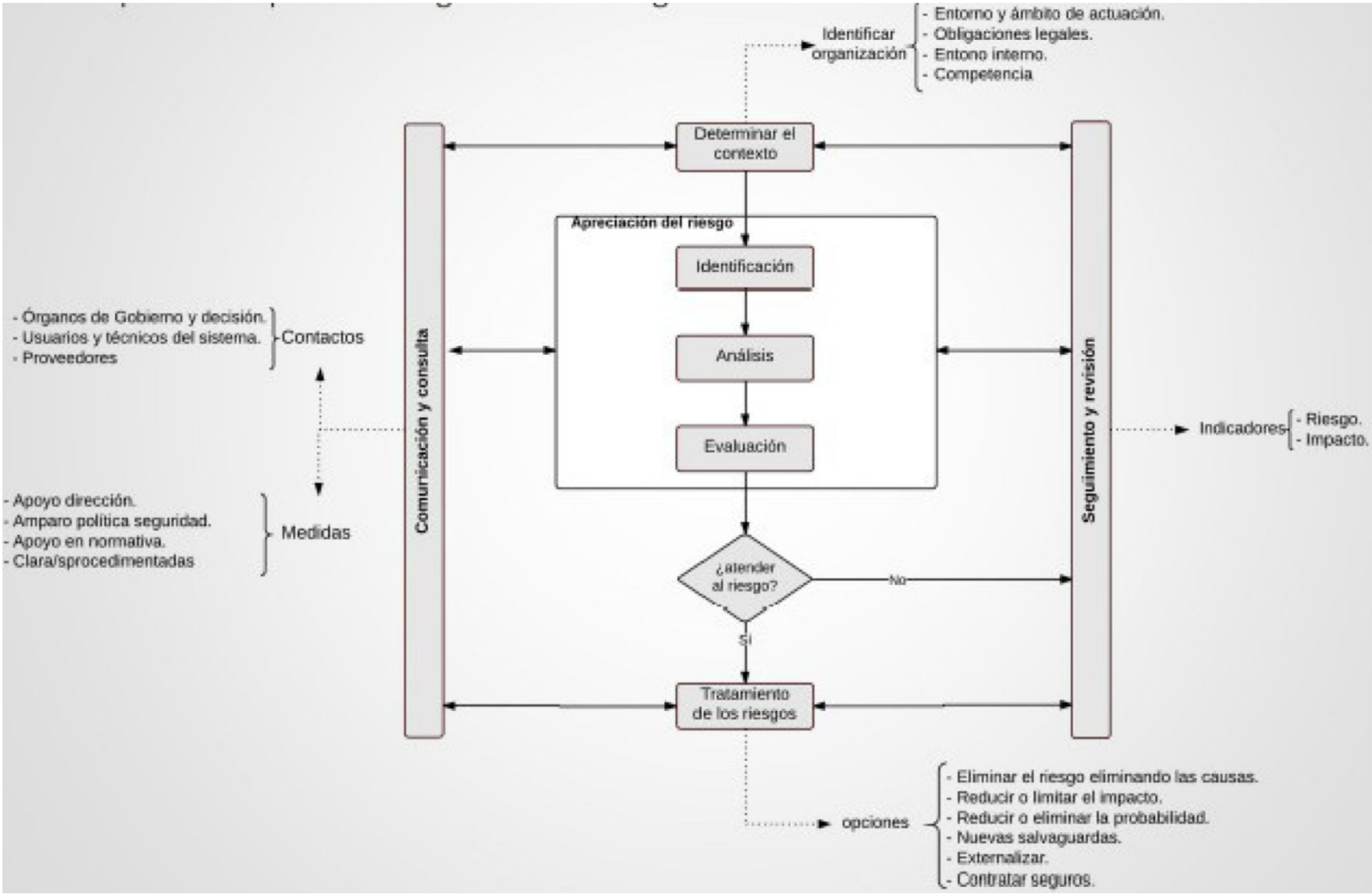
MAR – Método de Análisis de Riesgos

- MAR.1 – Caracterización de los activos
  - MAR.11 – Identificación de los activos
  - MAR.12 – Dependencias entre activos
  - MAR.13 – Valoración de los activos
- MAR.2 – Caracterización de las amenazas
  - MAR.21 – Identificación de las amenazas
  - MAR.22 – Valoración de las amenazas
- MAR.3 – Caracterización de las salvaguardas
  - MAR.31 – Identificación de las salvaguardas pertinentes
  - MAR.32 – Valoración de las salvaguardas
- MAR.4 – Estimación del estado de riesgo
  - MAR.41 – Estimación del impacto
  - MAR.42 – Estimación del riesgo

Universidad Zaragoza

Introducción a MAGERIT

Esquema de gestión del riesgo



Universidad Zaragoza

Herramientas para análisis de riesgos

https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html

Herramientas EAR (Entorno de Análisis de Riesgos)

Disponibles para el ciudadano (CCN – Centro Criptológico Nacional)

Soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit

Desarrolladas y financiadas parcialmente por el CCN
Se actualizan periódicamente y existen distintas versiones:

PILAR: versión completa de la herramienta

PILAR Basic: versión sencilla para Pymes y Administración local

μPILAR: versión reducida de PILAR, destinada a la realización de análisis de riesgos muy rápidos

RMAT (Risk Management Additional Tools) Personalización de herramientas

Universidad Zaragoza
1542

Referencias y bibliografía

Libros de MAGERIT (versión 3)

https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en#.VGyw4-e-uFw

Universidad Zaragoza

Contexto normativo y gestión de riesgos

Grado en Ingeniería en Informática e Ingeniería de Tecnologías y Servicios de Telecomunicación

Curso 2023-2024

Raquel Trillo Lado (raqueltl@unizar.es)

Carlos Tellería (telleria@unizar.es)

Fernando Tricas García (ftricas@unizar.es)

Dpto. Informática e Ingeniería de Sistemas