

Unidad 8: Escenarios particulares para realizar análisis

BLOQUE II – El análisis del ciberriesgo: enfoques cualitativos y cuantitativos

Grado en Ingeniería de la Ciberseguridad, curso 2022-2023

CONTENIDOS

1. Riesgos para la privacidad.
2. Riesgos en contextos cloud y nuevos paradigmas.

1. Riesgos para la privacidad

- Hasta hace relativamente poco tiempo, en proyectos/sistemas en los que se manejaban datos personales se realizaba la gestión de riesgos con metodologías y herramientas clásicas en ciberseguridad.
 - Haciendo especial énfasis en la confidencialidad, la integridad y el control de acceso.
 - Y en los activos asociados a la información

1. Riesgos para la privacidad

- Pero este enfoque presenta limitaciones importantes:
 - No está orientado al cumplimiento de legislación y normativa.
 - No suele tener en cuenta el factor humano de manera específica.
 - No tiene en cuenta los flujos de datos ni las actividades que se realizan con ellos en cada etapa del proyecto/sistema.
- Por lo que en los últimos años se están haciendo esfuerzos para proponer metodologías y herramientas específicas.
 - Y estándares, marcos de trabajo (recuerda la unidad 3).

1. Riesgos para la privacidad

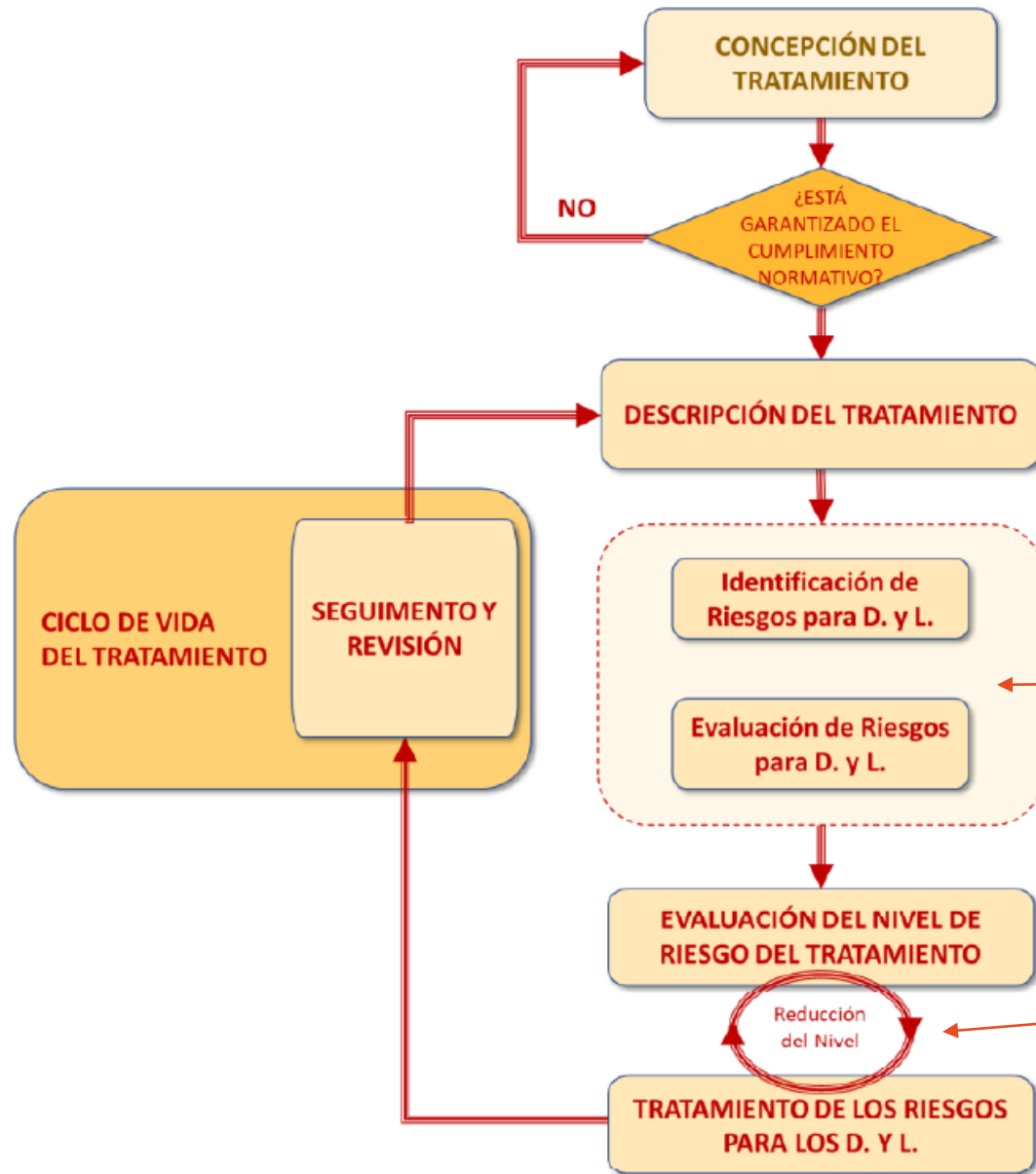
- Aspectos en común de estas nuevas propuestas:
 - Tienen en cuenta desde las primeras fases del análisis de riesgos el cumplimiento de legislación y normativa que afecta al proyecto/sistema en cuanto a privacidad y protección de datos.
 - Tienen en cuenta el factor humano de manera específica.
 - Impactos para las personas (derechos y libertades), no sólo técnicos o financieros.
 - Tienen en cuenta los flujos de datos y las actividades que se realizan con ellos en cada etapa del proyecto/sistema.
 - Para ello suelen servirse de casos de uso, mapas de flujo y diferentes herramientas gráficas.

1. Riesgos para la privacidad

- Aparecen conceptos como el de Privacy Impact Assessment (PIA) ó Evaluación de Impacto para la Protección de Datos (EIPD).
- El GDPR obliga a realizar EIPD antes de realizar cualquier tratamiento en el que sea probable que exista un alto riesgo para los derechos y libertades de los afectados: listado de la AEPD en <https://www.aepd.es/media/criterios/listas-dpia-es-35-4.pdf>
 - Es tarea del responsable del tratamiento, siempre en coordinación con el DPD y con el encargado del tratamiento.
 - Esta evaluación se debe repetir cuando se produzcan cambios en los riesgos que se corren.

1. Riesgos para la privacidad





A un nivel más alto, luego detallando por fases/etapas y teniendo en cuenta el ciclo de vida de los datos.

Escalas para probabilidad e impacto y factores de riesgo detallados en las últimas guías.

Riesgo inherente vs riesgo residual. Catálogo de medidas y garantías en las últimas guías. Plan de acción.

1. Riesgos para la privacidad

¿Qué datos se van a tratar?

¿Qué se va a hacer con los datos y con qué finalidad? ¿No se podría hacer de otra manera?

¿Son necesarios todos ellos?

¿Se cumple el principio de minimización?

¿De quién son los datos que se tratan?

**¿El tratamiento es
lícito?**

**¿El tratamiento es
proporcional?**

¿El tratamiento es lícito?



- Consentimiento del interesado para los fines específicos del tratamiento.
- El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte.
- El tratamiento es necesario para el cumplimiento de una obligación legal.
- El tratamiento es necesario para proteger intereses vitales de una persona física.
- El tratamiento es necesario para el cumplimiento de una misión realizada por el interés público.
- El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable.

¿El tratamiento es proporcional?



- Juicio de idoneidad: Consigue el objetivo propuesto.
- Juicio de necesidad: Es necesario, no existe otra forma de conseguir lo mismo con la misma eficacia.
- Juicio de proporcionalidad en sentido estricto: Se derivan más beneficios o ventajas para el interés general que no perjuicios.

DESCRIPCIÓN DEL TRATAMIENTO			
Su propósito	Su naturaleza	Su ámbito/ alcance ⁴⁶	Su contexto
<ul style="list-style-type: none"> • Fines últimos. • Fines instrumentales. • Fines secundarios. • Otros... 	<ul style="list-style-type: none"> • Las etapas en las que se implementa. • El flujo de datos personales. • Las operaciones de tratamiento que precisa (manuales y automatizadas). • Los activos/ elementos sobre los que se implementa. • Los roles que acceden a los datos. • Las características tecnologías relevantes. • La participación de encargados en distintas operaciones. • Otros... 	<ul style="list-style-type: none"> • La extensión en la cantidad de datos. • La extensión en la cantidad de sujetos afectados. • La extensión en los tipos y categorías de datos. • La extensión geográfica. • La extensión en el tiempo del tratamiento. • La extensión en el tiempo de la conservación. • La frecuencia de recogida. • La granularidad. • Otros... 	<ul style="list-style-type: none"> • El mercado o sector en el que se desenvuelve. • El entorno social en el que despliega. • El entorno normativo. • La interacción con otros tratamientos de la entidad. • Las cesiones de datos que son necesarias. • Las transferencias internacionales que implica. • Las brechas de seguridad o incidentes que se producen en tratamientos relacionados. • Los efectos colaterales en la sociedad • Otros...

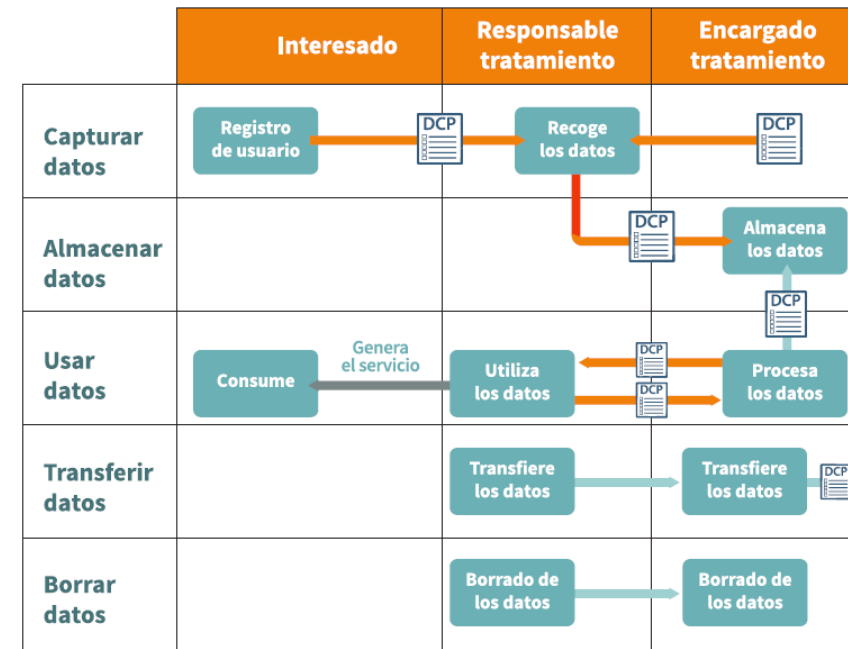
1. Riesgos para la privacidad



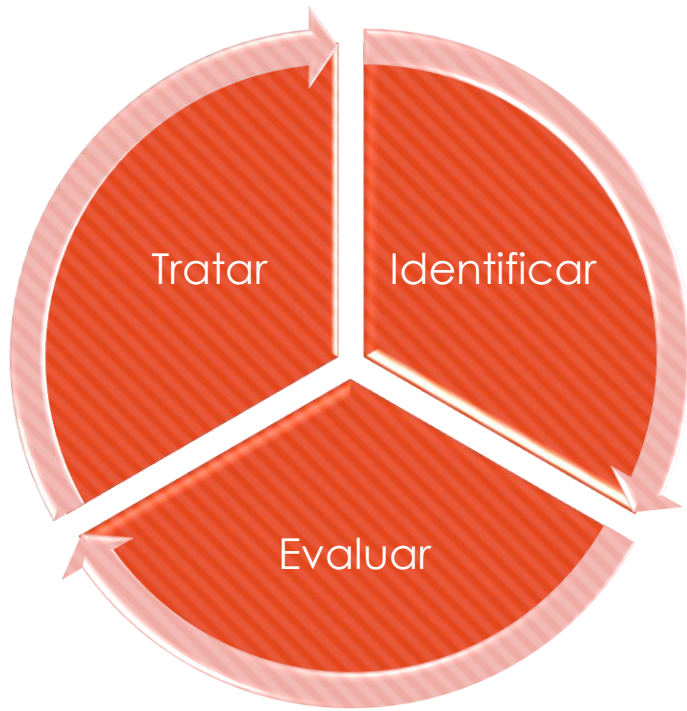


- 1 Captura de datos:** Proceso de obtención de datos para su almacenamiento y posterior procesado. Dentro de esta categoría se pueden encontrar diversas técnicas: formularios web, formularios en papel, toma de muestras y realización de encuestas, grabaciones de audio y video, redes sociales, captación mediante sensores, etc.
- 2 Clasificación / Almacenamiento:** Establecer categorías y asignarlas a los datos para su clasificación y almacenamiento en los sistemas o archivos.
- 3 Uso / Tratamiento:** Operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos de los datos automatizados o manuales.
- 4 Cesión o transferencia de los datos a un tercero para su tratamiento:** Traspaso o comunicación de datos realizada a un tercero, definido como aquella persona física o jurídica, pública o privada u órgano administrativo. Este concepto es muy amplio, puesto que recoge tanto la entrega, comunicación, consulta, interconexión, transferencia, difusión o cualquier otra forma de acceso a los datos.
- 5 Destrucción:** Eliminar los datos que puedan estar contenidos en los sistemas o archivos, de manera que no puedan ser recuperados de los soportes de almacenamiento.

		ETAPAS				
		Captura de datos	Clasificación / Almacenamiento	Uso / Tratamiento	Cesión o transferencia de los datos a un tercero	Destrucción
ELEMENTOS	Actividades del proceso					
	Datos tratados					
	Intervinientes involucrados					
	Tecnologías intervinientes					



1. Riesgos para la privacidad



$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$

Probabilidad	Impacto			
	Despreciable · 1	Limitada · 2	Significativa · 3	Máxima · 4
Máxima 4	4	8	12	16
Significativa 3	3	6	9	12
Limitada 2	2	4	6	8
Despreciable 1	1	2	3	4

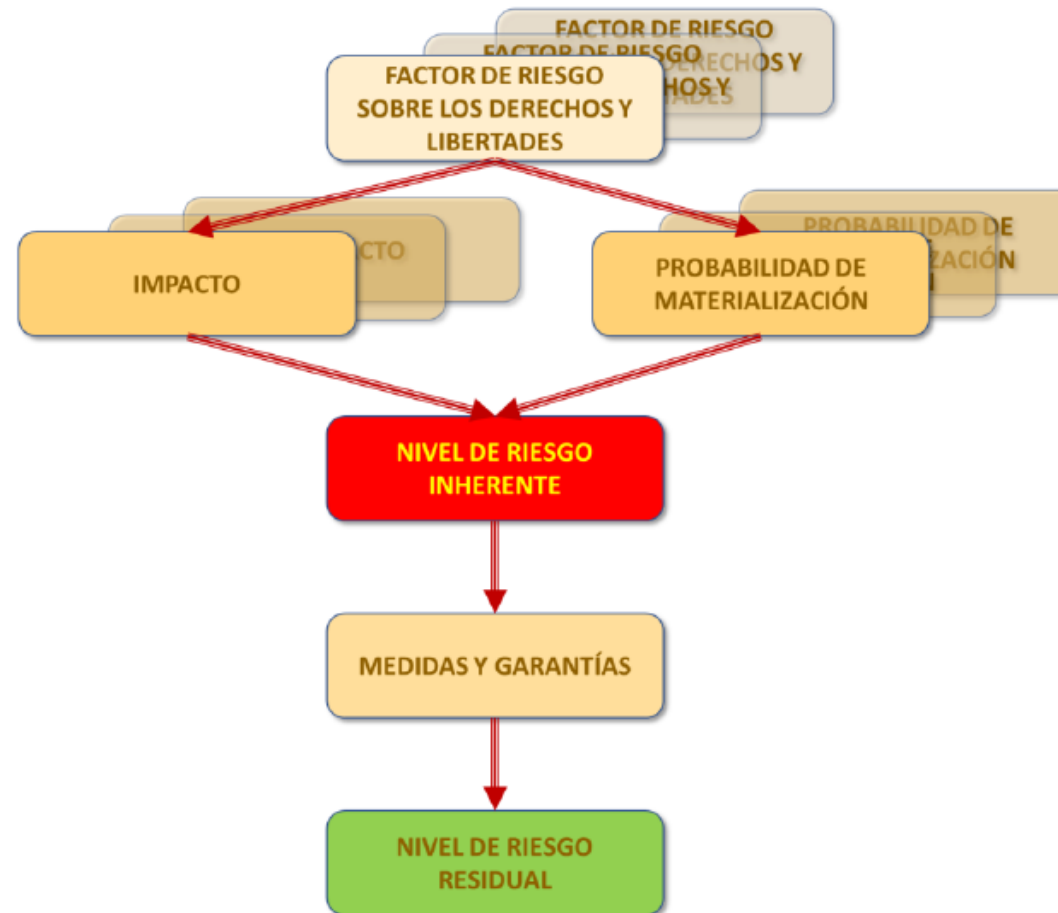
Legend:
□ Bajo (White)
■ Alto (Orange)
■ Medio (Yellow)
■ Muy Alto (Red)

1. Riesgos para la privacidad

Tratamiento
de los
riesgos
(plan de
acción)

- Conjunto de iniciativas que se deben llevar a cabo para implantar los controles que ayudan a reducir el riesgo de una actividad de tratamiento hasta un nivel considerado aceptable. Debe incluir, como mínimo, la descripción de cada control, el responsable de su implantación y el plazo de implantación.

1. Riesgos para la privacidad



1. Riesgos para la privacidad

- La AEPD distingue entre riesgo inherente y riesgo residual, y esto es muy importante a la hora de realizar las evaluaciones de impacto.
 - El riesgo inherente a la realización de un tratamiento es el que se observa cuando no lo gestionamos, cuando no aplicamos ningún tipo de control.
 - El riesgo residual es que el ser observa cuando aplicamos los controles que creemos más adecuados: medidas y garantías.
- Obviamente, si lo hacemos bien, el riesgo residual siempre es menor que el inherente.

1. Riesgos para la privacidad

- Si la conclusión de la evaluación de impacto es favorable, la actividad de tratamiento se puede llevar a cabo, siempre y cuando, las medidas de control recogidas en el plan de acción se implanten adecuadamente
- Si la conclusión de la evaluación no es favorable (porque los riesgos residuales siguen siendo altos), se debe analizar la posibilidad de incluir medidas de control.
- Si no fuese posible el tratamiento no se podría llevar a cabo y sería necesario activar el procedimiento de consulta previa a la Autoridad de Control.

2. Riesgo en contextos cloud y nuevos paradigmas

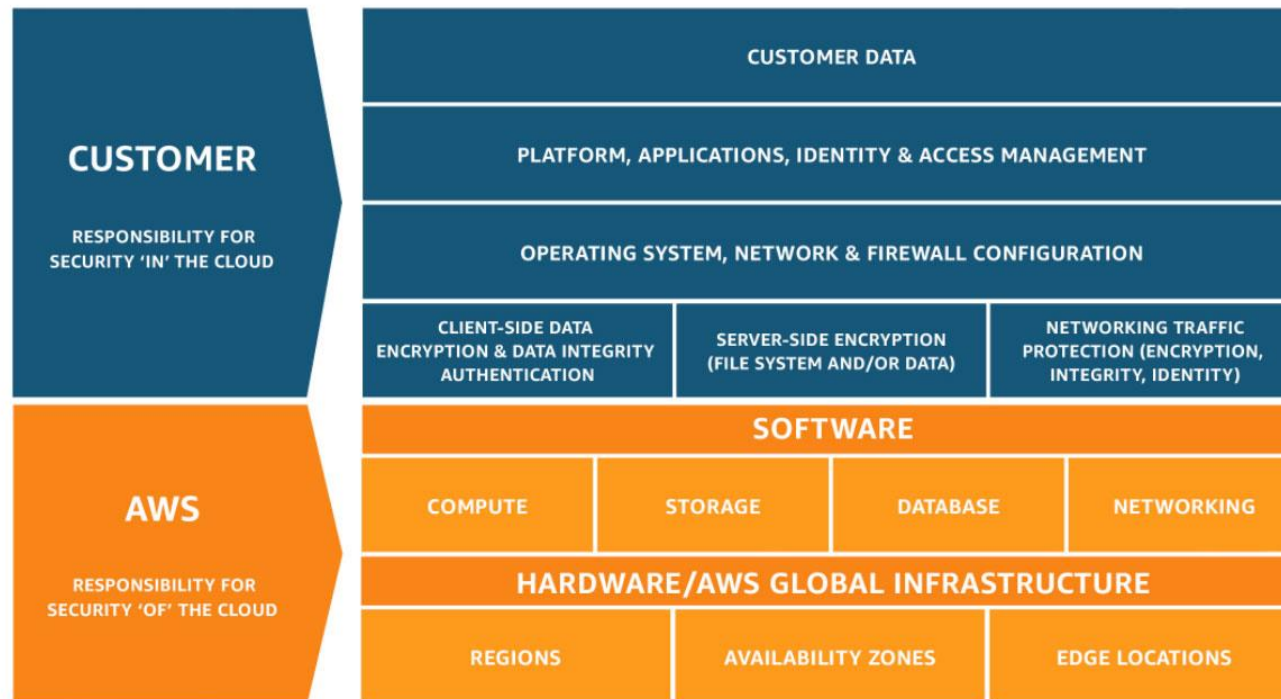
- Muchos problemas de seguridad y privacidad cuando se trabaja en la nube están provocados por intentar mantener los modelos, arquitecturas y controles clásicos.
 - Basados en la fortificación, el bastionado, la protección del perímetro, la segmentación de redes, etc.
- También con una falta de conocimiento de las responsabilidades de cada parte, con la ausencia de estándares/certificaciones y con una dificultad inherente para la monitorización.

2. Riesgo en contextos cloud y nuevos paradigmas

	IaaS	PaaS	SaaS
Gobernanza, cumplimiento, gestión del riesgo	Cliente	Cliente	Cliente
Seguridad de los datos	Cliente	Cliente	Cliente
Seguridad de la aplicación	Cliente	Cliente	Proveedor
Seguridad de la plataforma	Cliente	Compartida	Proveedor
Seguridad de la red y la infraestructura	Proveedor	Proveedor	Proveedor
Seguridad física	Proveedor	Proveedor	Proveedor

2. Riesgo en contextos cloud y nuevos paradigmas

○ Por ejemplo, del modelo de Amazon.



2. Riesgo en contextos cloud y nuevos paradigmas

- Existen una gran cantidad de estándares, recomendaciones y mejores prácticas que se pueden aplicar en cada una de las capas y según la responsabilidad.
 - ISO, NIST, DMTF, etc.
 - Además está todo el trabajo realizado específicamente para cada proveedor.
- Pero no hay metodologías de análisis de riesgos específicas, se trata de comprender los riesgos específicos y de adaptarse un poco al contexto.

2. Riesgo en contextos cloud y nuevos paradigmas

○ CSA = Cloud Security Alliance



2. Riesgo en contextos cloud y nuevos paradigmas

○ Iniciativas que es muy recomendable conocer y seguir:

Top Threats to Cloud Computing:
Egregious Eleven

Security Guidance
v4.0

Cloud Control Matrix
(CCM)

Consensus
Assessment Initiative
Questionnaire
(CAIQ) v3.1

2. Riesgo en contextos cloud y nuevos paradigmas

Data Breaches

Misconfiguration and inadequate change control

Lack of cloud security architecture and strategy

Insufficient identity, credential, access and key management

Account hijacking

Insider threat

Insecure interfaces and APIs

Weak control plane

Metastructure and applistrucre failures

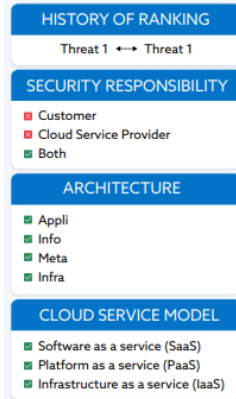
Limited cloud usage visibility

Abuse and nefarious use of cloud services

1. Security Issue: Data Breaches



A data breach is a cybersecurity incident where sensitive, protected or confidential information is released, viewed, stolen or used by an unauthorized individual. A data breach may be the primary objective of a targeted attack or merely the result of human error, application vulnerabilities or inadequate security practices. A data breach involves any kind of information that was not intended for public release, including—but not limited to—personal health information, financial information, personally identifiable information (PII), trade secrets and intellectual property.



Business Impact

Negative consequences of a data breach may include:

1. Impact to reputation and trust of customers or partners
2. Loss of intellectual property (IP) to competitors, which may impact products release
3. Regulatory implications that may result in monetary loss
4. Brand impact which may cause a market value decrease due to previously listed reasons
5. Legal and contractual liabilities
6. Financial expenses incurred due to incident response and forensics

There are cases of data breaches being undetected until months after the compromise. In such incidents, the implications might not be immediately apparent (e.g., IP theft). For example, the United States Office of Personnel Management (OPM) and Sony Pictures breach both had a dwell time of approximately one year¹.

Key Takeaways

1. Data are becoming the main target of cyber attacks. Defining the business value of data and the impact of its loss is important for organizations that own or process data.
2. Protecting data are evolving into a question of who has access to it.
3. Data accessible via the internet are the most vulnerable asset to misconfiguration or exploitation.
4. Encryption techniques can help protect data, but negatively impact system performance while making applications less user-friendly.
5. A robust and well-tested incident response plan that considers the CSP and data privacy laws will help data breach victims recover.

Anecdotes and Examples

- Timehop had a data breach that affected 21 million users because of a cloud computing environment compromise. Social media access tokens were also compromised.
- Uber disclosed that its Amazon Web Services (AWS) account was hacked in late 2016, compromising the personal information of 57 million users worldwide.
- In 2019, Voipio, a telecoms company that provides Voice over Internet Protocol (VoIP) services, exposed millions of customer call logs, short message service (SMS) logs and credentials. The database was exposed in June 2018 and contained call and message logs dating back to May 2015. Many of the files contained detailed call records (i.e., who called whom, time of call, etc.). In total, Voipio exposed “7 million call logs, 6 million text messages and other internal documents containing unencrypted passwords that— if used—could allow an attacker to gain deep access to the company’s systems.

CSA Security Guidance

Domain 2: Governance and Enterprise Risk Management
Domain 3: Legal Issues, Contracts and Electronic Discovery
Domain 4: Compliance and Audit Management
Domain 5: Information Governance
Domain 6: Management Plane and Business Continuity
Domain 9: Incident Response
Domain 11: Data Security and Encryption
Domain 12: Identity Entitlement and Access Management
Domain 14: Related Technologies

CCM Controls

AIS Application and Interface Security
AIS-01: Application Security
AIS-02: Customer Access Requirements
AIS-03: Data Integrity
AIS-04: Data Security / Integrity

EKM Encryption and Key Management
EKM-01: Entitlement
EKM-02: Key Generation
EKM-03: Sensitive Data Protection
EKM-04: Storage and Access

CCC Change Control and Configuration Management
CCC-05: Production Changes

GRM Governance and Risk Management
GRM-02: Data Focus Risk Assessments
GRM-06: Policy
GRM-10: Risk Assessments

DSI Data Security and Information Lifecycle Management
DSI-01: Classification
DSI-02: Data Inventory / Flows
DSI-03: Ecommerce Transactions
DSI-04: Handling / Labeling / Security Policy
DSI-05: Non-Production Data
DSI-07: Secure Disposal

IAM Identity and Access Management
IAM-01: Audit Tools Access
IAM-04: Policies and Procedures

2. Riesgo en contextos cloud y nuevos paradigmas

- Para mitigar estas amenazas la CSA proporciona unas guías o mejores prácticas en su Security Guidance.
 - Actualmente en su versión 4.
- Como en otros muchos marcos de trabajo, para no abrumar a quien lo tiene que aplicar, se trabaja por dominios.
 - Catorce en total.

DOMINIO 1

Conceptos y Arquitecturas de la Computación en la Nube



DOMINIO 2

Gobierno y Gestión del Riesgo Corporativo



DOMINIO 3

Cuestiones Legales, Contratos y Descubrimiento Electrónico



DOMINIO 4

Cumplimiento y Gestión de Auditoría



DOMINIO 5

Gobierno de la Información



DOMINIO 6

Plano de Gestión y Continuidad del Negocio



DOMINIO 7

Seguridad de la Infraestructura



DOMINIO 8

Virtualización y Contenedores



DOMINIO 9

Respuesta ante Incidentes



DOMINIO 10

Seguridad de Aplicaciones



DOMINIO 11

Seguridad y Cifrado de Datos



DOMINIO 12

Gestión de Identidades, Derechos y Accesos



DOMINIO 13

Seguridad como Servicio



DOMINIO 14

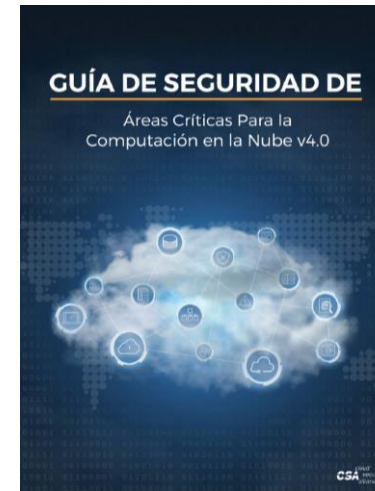
Tecnologías Relacionadas



2. Riesgo en contextos cloud y nuevos paradigmas

- La documentación es muy extensa y la podéis encontrar en GitHub o en distintos formatos de archivo.
 - Incluso traducida al español.

<https://github.com/cloudsecurityalliance/CSA-Guidance>



- Vamos a centrarnos en los aspectos relativos a los dominios más “técnicos”.

2. Riesgo en contextos cloud y nuevos paradigmas


CCM Domains

A&A	Audit & Assurance	IAM	Identity & Access Management
AIS	Application & Interface Security	IPY	Interoperability & Portability
BCR	Business Continuity Mgmt & Op Resilience	IVS	Infrastructure & Virtualization
CCC	Change Control & Configuration Management	LOG	Logging and Monitoring
CEK	Cryptography, Encryption and Key Management	SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
DCS	Datacenter Security	STA	Supply Chain Mgmt, Transparency & Accountability
DSP	Data Security and Privacy	TVM	Threat & Vulnerability Management
GRM	Governance, Risk Management and Compliance	UEP	Universal EndPoint Management
HRS	Human Resources Security		

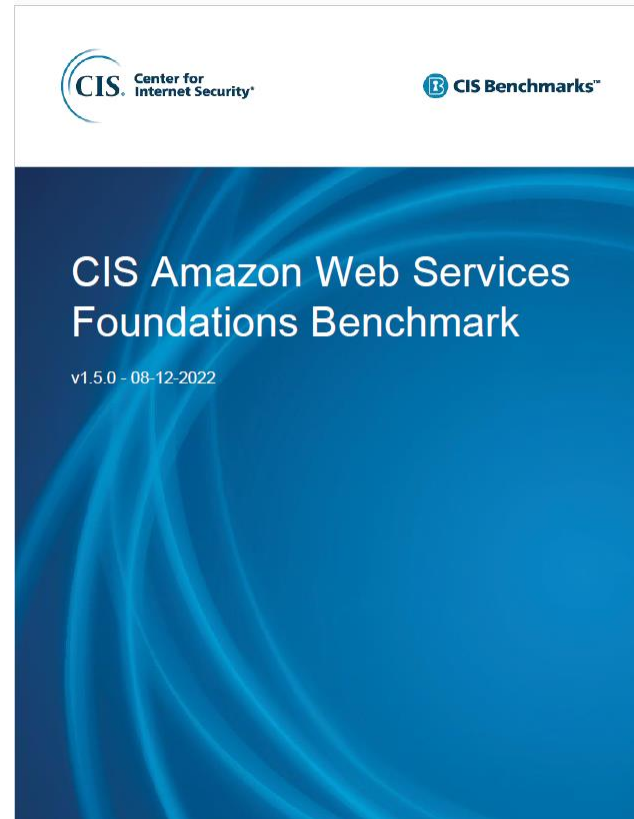
2. Riesgo en contextos cloud y nuevos paradigmas

CCM™ CLOUD CONTROLS MATRIX v4.0.6				
Control Domain	Control Title	Control ID	Control Specification	Auditing Guidelines
Audit & Assurance - A&A				
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	<ol style="list-style-type: none"> 1. Examine policy and procedures to confirm content adequacy in terms of purpose, authority and accountability, responsibilities, planning, communication, reporting, and follow-up. 2. Examine audit charter and determine if independence, impartiality, and objectivity are guaranteed. 3. Examine policy and procedures for evidence of review at least annually.
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	<ol style="list-style-type: none"> 1. Examine the process to determine standards and regulations applicable to the organization's systems and environments. 2. Determine if the organization maintains and reviews a list of such standards and regulations. 3. Determine if senior management exercises oversight over the independence of the assessment process. 4. Determine if the audit plan is informed by previous assessments, and is scheduled on an annual basis.
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	<ol style="list-style-type: none"> 1. Examine the process for determining the risks applicable to the organization's systems and environments. 2. Determine if a list of such risks is maintained and reviewed. 3. Determine if senior management exercises oversight over the applicable risks. 4. Determine if the audit plan is risk-based, and is scheduled on an annual basis.

2. Riesgo en contextos cloud y nuevos paradigmas

 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2							
Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?					A&A-01	Establish, document, and maintain audit and assurance policies and procedures.
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?						
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?					A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?					A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?					A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.
	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules,						Define and implement an audit management process to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules,

2. Riesgo en contextos cloud y nuevos paradigmas



<https://www.cisecurity.org/cis-benchmarks>

2. Riesgo en contextos cloud y nuevos paradigmas

- Este mismo ejercicio de búsqueda, documentación, investigación y análisis lo tenéis que realizar para otros contextos específicos en los que se usan nuevos paradigmas:
 - IoT, edge, fog.
 - 5G.
 - Blockchain.
 - Etc.

Para leer e investigar...

- “Guía de Gestión de riesgo y evaluación de impacto en tratamientos de datos personales”, AEPD (2021).
- Herramienta **GESTIONA** **EIPD**
<https://gestion.aepd.es/>

Referencias

- Fotografías

- <https://unsplash.com>

- Iconos

- <https://www.flaticon.es/>



**Reconocimiento-CompartirIgual 3.0
España (CC BY-SA 3.0 ES)**

©2023 Marta Beltrán URJC (marta.beltran@urjc.es)

Algunos derechos reservados.

Este documento se distribuye bajo la licencia “Reconocimiento-CompartirIgual 3.0 España” de Creative Commons, disponible en

<https://creativecommons.org/licenses/by-sa/3.0/es/>