






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

Ejemplos prácticos de amenazas y su relación con el riesgo y su posible impacto:

 **Ejemplo nº1 (acceso ilegítimo a los datos):** La pérdida de un dispositivo móvil o la fuga de información (**Amenaza**), podría derivar en un acceso por parte de personal no autorizado a los datos y, en consecuencia, se produciría una vulneración de los derechos y libertades de los interesados (**riesgo**), lo que podría derivar en un posible daño moral, físico o material sobre el interesado (**Impacto**).





 **Ejemplo nº2 (modificación no autorizada de los datos):** La ausencia de mecanismos de control en un sistema es una vulnerabilidad que puede facilitar una suplantación de identidad derivada de un ataque cibernético (**amenaza**). El ataque puede provocar una modificación no autorizada de datos que altere la integridad y disponibilidad de los datos (**riesgo**), con la posibilidad de provocar daños y perjuicios, materiales a los interesados (**impacto**).

 **Ejemplo nº3 (eliminación de los datos):** Un fallo en el suministro eléctrico o un desastre natural pueden provocar una pérdida de datos (**amenaza**), que podría derivar en la falta de disponibilidad de los datos para una determinada operación de tratamiento (**riesgo**), con la posibilidad de provocar daños y perjuicios, materiales a los interesados (**impacto**).

	Etapas del ciclo de vida de los datos	Amenaza identificada	Riesgo	Impacto
Ejemplo nº1	Almacenamiento de los datos	Pérdida de un dispositivo móvil o fuga de información	Vulneración de los derechos y libertades	Daño moral, físico o material
Ejemplo nº2	Uso / tratamiento de los datos	Ataque cibernético para la suplantación de identidad	Modificación no autorizada de datos	Daños materiales a los interesados
Ejemplo nº3	Uso / tratamiento de los datos	Fallo en el suministro eléctrico o desastre natural	Borrado o pérdida de datos	Daños materiales a los interesados



Ejemplos de posibles daños físico, material o moral

 Despreciable: Los interesados no se verán prácticamente afectados o encontrarán alguna pequeña inconveniencia	<ul style="list-style-type: none">■ Molestias o irritación.■ Se incumplen obligaciones materiales sin perjuicios relevantes.■ No se priva de los derechos y libertades.
 Limitado: Los interesados podrán encontrar inconveniencias no significativas	<ul style="list-style-type: none">■ Estrés o padecimientos físico menores.■ Costes extra, denegación de acceso a algunos servicios o incumplimiento de obligaciones materiales con perjuicios económicos.■ Se priva de los derechos y libertades de los interesados, por ejemplo, por difamación de un interesado por divulgación de datos personales.
 Significativo: Los interesados encontrarán consecuencias significativas, que deberían poder superar sin dificultades serias.	<ul style="list-style-type: none">■ Empeoramiento del estado de salud o agresiones físicas.■ Apropiación indebida de fondos, pérdida del empleo o incumplimiento de obligaciones materiales con perjuicios económicos relevantes.■ Se agrede contra los derechos y libertades de los interesados, por ejemplo, una citación judicial, entrar en una lista de morosidad o divulgación de datos personales con impacto significativo en la reputación del interesado.
 Máximo: Los interesados encontrarán consecuencias significativas o incluso irreversibles, que podrán no llegar a superarse.	<ul style="list-style-type: none">■ Agresiones físicas con consecuencias irreparables.■ Asunción de una deuda inabordable, imposibilidad de volver a trabajar o incumplimiento de obligaciones materiales con perjuicios económicos irreparables.■ Se agrede significativamente contra los derechos y libertades de los interesados, por ejemplo, padecimiento psicológico con consecuencias a largo plazo o irreparables por la divulgación de datos sensibles.



- 1 Despreciable
- 2 Limitado
- 3 Significativo
- 4 Máximo

Si se enfrentan la probabilidad y el impacto, se forma una matriz de riesgo, tal y como se puede ver a continuación:

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

- ☐ Bajo
- ☐ Medio
- ☐ Alto
- ☐ Muy Alto

Supongamos una aplicación móvil con almacenamiento en la nube que captura datos a través de *weareables* (dispositivos como un reloj o pulsera), además de permitir la introducción manual de datos de salud por parte del usuario. La finalidad de la actividad de tratamiento es monitorizar la actividad del usuario y recomendar hábitos de vida saludables. La aplicación móvil no dispone de medidas de control de acceso, ni de detección de malware, además no se realizan copias de seguridad de los datos. Adicionalmente, durante la fase de registro del usuario no se solicita consentimiento expreso para ninguna finalidad adicional a la mencionada.

Ante este contexto, se puede identificar, entre otras, varias amenazas y riesgos asociados que se describen y evalúan a continuación:

Tipo amenaza	Amenaza	Riesgo	Probabilidad	Impacto	Riesgo inherente
Acceso ilegítimo a los datos	Fuga de información (derivada de la pérdida del dispositivo móvil)	Acceso no autorizado por parte de terceros a datos de salud (violación de la confidencialidad)	Significativa 3	Significativo 3	Alto 9
	Operación de tratamiento no autorizada (derivada del uso de los datos para una finalidad sin base legítima, por ejemplo, acciones de marketing indirecto sobre productos de salud)	Uso ilegítimo de datos personales (vulneración de los derechos y libertades)	Máxima 4	Limitado 2	Alto 8
Modificación no autorizada de los datos	Ataque cibernético (malware que modifica los datos almacenados en la nube)	Modificación de datos no autorizada por parte de terceros (violación de la integridad)	Significativa 3	Limitado 2	Medio 6
	Operación de tratamiento no autorizada (derivada de una decisión automatizada en base al perfilado de datos erróneo por una mala programación del software , por ejemplo, una categorización de personas saludables con acceso a determinadas coberturas de un seguro de salud)	Uso ilegítimo de datos personales (vulneración de los derechos y libertades)	Máxima 4	Significativo 3	Muy alto 12
Eliminación de los datos	Corte de suministro eléctrico o fallos en servicios de comunicaciones (como consecuencia del fallo se produce un periodo temporal en el cual los datos no han sido almacenados)	Pérdida de datos almacenados en el sistema (violación de la disponibilidad)	Limitada 2	Limitado 2	Medio 4
	Ataque intencionado que provoca la indisponibilidad de los datos (como consecuencia de un ataque de cifrado de las bases de datos que inhabilita las mismas)	Pérdida de datos almacenados en el sistema (violación de la disponibilidad)	Significativa 3	Significativo 3	Alto 9