|  |  |
| --- | --- |
| PRIVACIDAD POR DEFECTO | |
| **Objetivo:** Conseguir una visión completa del diseño de las aplicaciones pensando en la privacidad. | |
| **Dinámica:** Realizar un estudio sobre las decisiones de diseño de una app concreta proporcionada por el profesor. | |
| **ESTA FICHA TIENE EQUIPO RECORDER** | |
| **Grupo** | **Fecha** |
|  |  |
| **Roles** | **Nombre y Apellidos** |
| **Recorder:** Contesta las preguntas en el papel siguiendo las indicaciones del grupo. |  |
| **Speaker:** Habla en la puesta en común. Puede realizar preguntas al profesor |  |
| **Manager:** Gestiona el trabajo y se encarga de que el trabajo pueda ser entregado a tiempo. Sería el encargado de entregar un informe de equipo si el trabajo no se ha finalizado a tiempo. |  |
| **Auditor**: Observa la actividad del grupo, avisa si se está desviando el objetivo del trabajo/tiempo de entrega.  Conviene que controle el tiempo asignado a la actividad, por ejemplo, con el móvil |  |
| **Contributor 1:** Ayuda a contestar las preguntas, buscando información y aportando ideas y sugerencias. |  |
| ***Contributor 2*** |  |

## XI. ANEXO II: LISTA DE OPCIONES DE CONFIGURACIÓN

Lista, no exhaustiva y con carácter orientativo, de aquellas opciones en las que un tratamiento podría ser configurable para implementar las medidas con relación a la cantidad de datos personales utilizados, la extensión del tratamiento, el periodo de conservación, la accesibilidad de los datos y cualquier otra circunstancia en el proceso del tratamiento susceptible de incidir en la privacidad de los usuarios.

Basado en: <https://www.aepd.es/guias/guia-proteccion-datos-por-defecto.pdf>

|  |  |  |  |
| --- | --- | --- | --- |
| **Opciones de configuración agrupadas por tipo de medida** | *Indicar cual es la configuración por defecto* | *Indicar si está activado o desactivado* |  |
| **Extensión del tratamiento** | **Configurable** | **No configurable** | **No aplica** |
| Operación en modo anónimo. |  |  |  |
| Operación sin necesidad de crear cuenta de usuario. |  |  |  |
| Operación con distintas cuentas de usuario sobre el mismo dispositivo para el mismo interesado. |  |  |  |
| Operación con distintas cuentas de usuario sobre distintos dispositivos para el mismo interesado y tratamiento. |  |  |  |
| Identificación mediante herramientas y tecnologías que refuerzan la privacidad como las credenciales basadas en atributos, las pruebas de conocimiento cero, … |  |  |  |
| Agregación de datos: en el tiempo, en el espacio, por colectivos… |  |  |  |
| Calibración de la granularidad de los datos: p.ej. disminuir la frecuencia de recogida de datos de localización, de medida, etc.. |  |  |  |
| Generalización de los datos: emplear rangos para edad, direcciones postales para direcciones. |  |  |  |
| Graduación de la extensión de los datos recogidos en función de los casos de uso |  |  |  |
| Alternativas y voluntariedad en la información de contacto reclamada al usuario: email, postal, teléfono… |  |  |  |
| Técnicas de seguimiento en el tratamiento (cookies, etiqueta de pixeles, fingerprint, etc.) |  |  |  |
| Configuración de identificadores unívocos (tracking IDs), la programación de su reinicialización y el aviso de tiempos de activación. |  |  |  |
| Metadatos del dispositivo recogidos del dispositivo (consumo de batería, S.O., versiones, lenguajes, etc.). |  |  |  |
| Metadatos incluidos en los soportes tratados o generados (en documentos, fotos, videos, etc.) |  |  |  |
| Información recogida sobre la conexión de internet del usuario (dispositivo con el que se conecta, dirección IP, datos de sensores del dispositivo, aplicación utilizada, registro de navegación y búsqueda, registro de fecha y hora de solicitud de página web, etc.) e información sobre elementos cercanos al dispositivo (puntos de acceso  Wi-Fi, antenas de servicio de telefonía móvil, dispositivos bluetooth activados, etc.). |  |  |  |
| Información recogida sobre la actividad del usuario en el dispositivo: encendido, activación de aplicaciones, uso de teclado, ratón, etc. |  |  |  |
| Mecanismos de recogida escalonada de la información necesaria para el tratamiento. Retrasar la recogida de datos hasta la fase en que sean necesarios. |  |  |  |
| Tipo y volumen de nuevos datos inferidos a partir de procesos automatizados como el machine learning u otras técnicas de inteligencia artificial. |  |  |  |
| Enriquecimiento de datos y la vinculación con conjuntos de datos externos |  |  |  |
| Activación y desactivación a voluntad de los sistemas de recogida de datos (cámaras, micrófonos, GPS, bluetooth, wifi, movimiento, etc.). |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Establecer una programación temporal de cuándo los sensores (p.ej. cámaras, micrófonos, etc.) pueden estar operativos. | |  | |  |  |
| Incorporación de mecanismos de ofuscación para evitar el tratamiento de datos biométricos en fotos, video, teclado, ratón, etc. | |  | |  |  |
| Bloqueadores físicos (como las pestañas para cubrir las lentes de las cámaras, bloqueadores de altavoces, etc.). | |  | |  |  |
| Utilización de máscaras de privacidad o pixelado en los sistemas de videovigilancia. | |  | |  |  |
| **Extensión del tratamiento** | | **Configurable** | | **No configurable** | **No aplica** |
| Definición y diseño de los tratamientos para minimizar la cantidad de copias temporales de datos que se generen y reducir al máximo los tiempos de conservación, las transferencias y comunicaciones | |  | |  |  |
| Seudonimización atendiendo a las operaciones de tratamiento que puedan existir en cada fase o etapa. | |  | |  |  |
| Procesamientos de carácter local y aislado, incluida la posibilidad de almacenamiento local. | |  | |  |  |
| Tratamiento adicional de los metadatos recogidos – ficheros log. | |  | |  |  |
| Ejercicio de derechos de oposición, limitación o supresión. | |  | |  |  |
| Configuración del tratamiento para perfilado o decisiones automáticas (caso cookies) | |  | |  |  |
| Posibilidad de configurar todas las operaciones optativas de tratamientos para finalidades no imprescindibles: por ejemplo, tratamiento de datos para mejora del servicio, análisis de uso, personalización de anuncios, detección de patrones de uso, etc. | |  | |  |  |
| Configuración de un borrado seguro de ficheros temporales, principalmente aquellos situados fuera del dispositivo del usuario y fuera de los sistemas del responsable | |  | |  |  |
| Incorporación de una opción de reinicialización de los datos de usuario para retomar la relación desde cero | |  | |  |  |
| Configuración de la opción de enriquecimiento de datos | |  | |  |  |
| Contemplar mecanismos para auditar la existencia de Dark Patterns | |  | |  |  |
| Apartado específico para las opciones de configuración relacionadas con datos sensibles | |  | |  |  |
| Panel de ayuda y transparencia con ejemplos de uso y posibles riesgos y consecuencias para los derechos y libertades del usuario | |  | |  |  |
| Incorporación de un medio específico (botón o enlace) de retorno a la configuración inicial con valores por defecto | |  | |  |  |
| **Periodo de almacenamiento** | | **Configurable** | **No configurable** | | **No aplica** |
| Configuración de borrado de datos de sesión tras su cierre. | |  | |  |  |
| Configuración de plazos máximos para el cierre de sesión en la aplicación o dispositivos. | |  | |  |  |
| Plazos de conservación de perfiles de usuario. | |  | |  |  |
| Configuración de la gestión de copias temporales. | |  | |  |  |
| Control del borrado de copias de temporales. | |  | |  |  |
| Eliminación del rastro del usuario en el servicio: “derecho al olvido”. | |  | |  |  |
| Identificación, dentro del registro de expedientes de datos recogidos de las secciones, o datos dentro de secciones, que puedan ser anonimizables. | |  | |  |  |
| Programación de mecanismos de bloqueo y borrado automático. | |  | |  |  |
| Programación de mecanismos automáticos de borrado de salidas a dispositivos de impresión. | |  | |  |  |
| Configuración de plazos de conservación de datos históricos en el servicio: p.ej., en los sitios de compra, últimos artículos, ultimas consultas, etc. | |  | |  |  |
| Incorporación de mecanismos genéricos de anonimización. | |  | |  |  |
| **Accesibilidad de los datos** |  | **Configurable** | | **No configurable** | **No aplica** |
| Información de perfil del interesado mostrada a usuario y terceros: nombre, pseudónimo, teléfono, etc. | |  | |  |  |
| Información del interesado que se muestra a terceros: p.ej. divulgación selectiva de elementos del CV, la historia clínica, etc. | |  | |  |  |
| Información de estatus del interesado accesible a terceros. P.ej. en las aplicaciones de mensajería, información sobre disponibilidad, escritura de mensaje, recepción de mensaje, lectura de mensaje, … | |  | |  |  |
| Clasificación y etiquetado de las operaciones de tratamiento, las secciones de los documentos y/o datos dentro de secciones, que puedan ser gestionados mediante una política de control de accesos. | |  | |  |  |
| Organización, clasificación y etiquetado de la aplicación o servicio de acuerdo con la sensibilidad de datos, secciones u operaciones de tratamiento. | |  | |  |  |
| Posibilidad de definición y configuración de perfiles de acceso y asignación granular de privilegios | |  | |  |  |
| Bloqueos automáticos de sesión. | |  | |  |  |
| Asignación de perfiles de acceso a los datos de acuerdo con los roles de los usuarios para cada fase del tratamiento. | |  | |  |  |
| Diseño del espacio de trabajo (zonas aisladas de entrevista, ficheros físicos no accesibles, carpetas no transparentes, pantallas no expuestas a terceros o con filtros de privacidad, cascos para los teléfonos, locutorios, políticas de mesas limpias, etc.) | |  | |  |  |
| Parámetros de gestión de la información como dónde se almacenan y procesan los datos, si se hace en claro o utilizando un sistema de cifrado, los mecanismos de control de acceso implementados, si existen múltiples copias de los datos, incluidas instancias borradas de forma no segura, que pueden ser accedidas por terceros. | |  | |  |  |
| Control del cifrado de almacenamiento de los datos | |  | |  |  |
| Control del cifrado de comunicación de los datos | |  | |  |  |
| Procedimientos de gestión de acceso a dispositivos compartidos de impresión/salida donde pueden quedar documentos abandonados por el usuario. | |  | |  |  |
| En su caso, prohibición de impresión. | |  | |  |  |
| Control del borrado de salidas de impresión | |  | |  |  |
| Procedimientos de gestión de dispositivos de almacenamiento portátil para su formateo periódico | |  | |  |  |
| La retención o eliminación de la información de sesión, en aplicaciones, sistemas compartidos, comunicaciones o sistemas proporcionados al empleado o al usuario final. | |  | |  |  |
| El tipo y cantidad de metadatos recogidos en la documentación generada por las utilidades del sistema (procesadores de texto, herramientas de dibujo, cámaras y videos, etc.) | |  | |  |  |
| En el envío de mensajes, configurar la incorporación de hilos de la conversación, así como configurar la posibilidad de confirmación de envío múltiples destinatarios. | |  | |  |  |
| Mecanismos de para evitar la indexación en Internet | |  | |  |  |
| Medidas organizativas y técnicas para revisión y filtrado de información que se va a hacer pública. | |  | |  |  |
| Sistemas de anonimización y/o seudonimización de textos a difundir. | |  | |  |  |
| Parámetros de gestión de los elementos de conectividad de los dispositivos (Wifi, Bluetooth, NFC, etc.). | |  | |  |  |
| Alertas sobre el estado de conectividad de los dispositivos. | |  | |  |  |
| Controles para evitar la comunicación de los identificadores unívocos del dispositivo (Advertising-ID, IP, MAC, número de serie, IMSI, IMEI, etc.) | |  | |  |  |
| Mecanismos de control de acceso a sistemas pasivos (como tarjetas contactless) con la incorporación de protocolos de autenticación de terminales o con medidas físicas para evitar el acceso electromagnético. | |  | |  |  |
| Controles de accesibilidad a contenidos del usuario en redes sociales. | |  | |  |  |
| Incorporación de controles para recoger acciones afirmativas y claras de confirmación antes de hacer públicos los datos personales, de forma que la diseminación esté bloqueada por defecto. | |  | |  |  |
| Configuración de avisos y recordatorios a los interesados sobre qué políticas de difusión y comunicación de la información están establecidas. | |  | |  |  |
| Definición y configuración de permisos de acceso sobre conjuntos de datos (bases de datos, sistemas de fichero, galerías de imágenes, …) y elementos de captación de información como sensores (cámaras, GPS, micrófonos, etc.) del dispositivo e información sobre elementos cercanos al dispositivo (puntos de acceso Wi-Fi, antenas de servicio de telefonía móvil, dispositivos bluetooth activados, etc.). | |  | |  |  |
| Definición y configuración de las políticas de permisos de acceso a datos entre aplicaciones y librerías, como en el caso de los teléfonos móviles. | |  | |  |  |
| Definición de perfiles de acceso en base a privilegios u otro tipo de barreras tecnológicas y procedimentales que impidan la vinculación no autorizada de fuentes de datos independientes. | |  | |  |  |
| Contenido registrado en los logs (quién, cuándo, a qué, qué acción, para qué propósito, … se accede a los datos). | |  | |  |  |
| Definición de sistemas automáticos de alerta ante eventos concretos. | |  | |  |  |
| Trazabilidad de la comunicación de datos entre responsables, encargados y subencargados. | |  | |  |  |
| Opciones de seguridad configurables (aparte de las opciones de cifrado). | |  | |  |  |
| Permitir configuraciones de acceso diferentes en función de distintos dispositivos. | |  | |  |  |
| Configurar sistemas de alerta por accesos anómalos a los datos. | |  | |  |  |
| Configuración de algunos de los parámetros de seguridad, en particular las claves y cómo balancear la relación seguridad/rendimiento/funcionalidad en función de la robustez deseada por el usuario. | |  | |  |  |
| Control del ámbito de distribución de la información que se distribuye en el entorno de la aplicación (redes sociales, redes laborales, etc.). | |  | |  |  |
| Configuración de la recepción de avisos cuando la información se está haciendo accesible a terceros. | |  | |  |  |
| Control de los metadatos incorporados en la información generada o distribuida. | |  | |  |  |
| Mecanismo del “derecho al olvido” de la información publicada en redes sociales u otros sistemas. | |  | |  |  |
| Opciones de elección respecto a dónde se almacenan los datos personales, ya sea en dispositivos locales o remotos y, en este último caso, otros parámetros como encargados o países. | |  | |  |  |
| Histórico de perfiles y entidades que han accedido a su información. | |  | |  |  |
| Información sobre el acceso a sus datos por usuarios autorizados | |  | |  |  |
| Información sobre los últimos cambios llevados a cabo y el perfil que ha realizado el cambio | |  | |  |  |
| Configurabilidad de controles de acceso por funcionalidades prestadas. | |  | |  |  |
| Configurabilidad de separación lógica de grupos de datos. | |  | |  |  |
| Configurabilidad de separación física de grupos de datos. | |  | |  |  |
| Deshabilitación o anulación selectiva de funcionalidades. | |  | |  |  |
| **General** | | **Configurable** | | **No configurable** | **No aplica** |
| En el caso de que el servicio sea multidispositivo, posibilidad (no obligación) de aplicar criterios generales de privacidad aplicable a todos ellos y en una única acción. | |  | |  |  |
| Recordatorios, iconos y avisos de todas aquellas acciones que afectan a la privacidad de la información: cambios de configuración, acceso a los datos por parte de terceros como captura de video, sonido, posición, etc. | |  | |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NOMBRE DEL PATRON DE DISEÑO | OBJETIVO FINALIDAD | DATOS RECOGIDOS/DATOS PROCESADOS/PROCESOS DÓNDE SE VA A APLICAR | |
| [Ofuscación de medidas mediante agregación de ruido](https://privacypatterns.eu/#/patterns/added-noise-measurement-obfuscation/0-0-0-2-0-1-0-3-3-0-0-1-1-0-0-0) | Modifica las medidas detalladas de uso o cualquier otro atributo de un servicio mediante la adición de valores de ruido que enmascaren los datos reales con el objetivo de evitar deducir patrones y comportamientos por parte de un tercero no autorizado que intercepte la comunicación. |  | |
| [Agregación](http://privacypatterns.wu.ac.at:8080/catalog/) en el tiempo | Consiste en recopilar datos correspondientes a diferentes momentos temporales y procesar información de manera agregada para proteger la privacidad. |  | |
| [Privacidad diferencial](http://privacypatterns.wu.ac.at:8080/catalog/) | Mediante este patrón se modifica el resultado de las consultas añadiéndoles nuevos datos (ruido) extraídos aleatoriamente de una distribución generada a partir de los datos originales de modo que la estadísticamente dicha modificación tiene un efecto insignificante en los resultados del algoritmo que analiza los datos y sin embargo permite preservar la privacidad de los individuos. |  | |
| [Complemento de aseguramiento de la privacidad](https://privacypatterns.eu/#/patterns/trustworthy-privacy-plug-in/0-0-0-1-1-0-1-1-0-0-0-0-1-1-0-0) | En muchas ocasiones la prestación de un servicio requiere la toma de medidas detalladas y repetitivas que, evaluadas en el tiempo, pueden revelar un comportamiento y poner en riesgo la privacidad del interesado. Este complemento, agrega, de manera confiable, los valores detallados de los registros en el lado del usuario proporcionando la finalidad perseguida, pero ocultando los valores desagregados detallados. |  | |
| [Granularidad de ubicación dinámica](https://privacypatterns.eu/#/patterns/dynamic-location-granularity/0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0) | En el caso de servicios basados en la geolocalización (LBS) permite que la información de ubicación del usuario logre el k-anonimato reduciendo la precisión, pero manteniendo un equilibrio con la utilidad de la información necesaria para la prestación del servicio. |  | |
| [Gateway de agregación](https://privacypatterns.eu/#/patterns/aggregation-gateway/0-0-0-1-0-1-0-1-1-0-0-1-1-1-0-0) | Implementa el cifrado homomórfico, cifrando, agregando y descifrando posteriormente la información tratada. Operando sobre la información cifrada, es posible realizar tratamientos de medidas tomadas en distintos momentos temporales sobre un usuario, pero sin extrapolar un patrón de comportamiento. Trabaja con datos agregados sin tener acceso a la información individual. |  | |
| [Transmisión activa de presencia](https://privacypatterns.org/patterns/Active-broadcast-of-presence) | Permite al usuario decidir cuándo quiere compartir información de una manera activa, en particular, información asociada a su ubicación. Los ajustes de difusión de información no deben aplicarse de forma holística por defecto y en caso de duda debe solicitarse confirmación. |  | |
| [Consentimiento informado](https://privacypatterns.org/patterns/Obtaining-Explicit-Consent) | Para determinados tratamientos el responsable necesita recabar el consentimiento informado del usuario. La implementación de este patrón garantiza mostrar un aviso claro, conciso y comprensible antes de recoger los datos e iniciar el tratamiento de que, al usar el servicio, el usuario está consintiendo en el tratamiento de los datos necesario y conoce las posibles consecuencias. Los detalles completos deberían ser fácilmente accesibles de modo que el usuario tenga la oportunidad de elegir utilizar o no el servicio. |  | |
| [Enlaces privados](https://www.privacypatterns.org/patterns/Private-link) | En entornos en los que el responsable proporciona a los usuarios un servicio de almacenamiento de contenido, potencialmente pueden existir datos personales. Si el usuario desea compartir parte de este contenido, pero de forma limitada, implementar este patrón permite enviar un enlace privado a los interesados concediendo acceso a la información, pero sin necesidad de hacerlo totalmente público. |  | |
| [Políticas adheridas](https://privacypatterns.eu/#/patterns/sticky-policies/0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0) | Son políticas de privacidad leídas e interpretadas de forma automática y que acompañan a los datos comunicados a terceras partes para definir sus posibilidades de uso, limitaciones y las preferencias del usuario, mejorando así el control que este tiene sobre sus datos personales |  | |
| [Elección desagregada de funcionalidades](https://www.privacypatterns.org/patterns/Enable-Disable-Functions) | Con frecuencia, los responsables recopilan más datos de los estrictamente necesarios con el objetivo de proporcionar funcionalidades adicionales con respecto a la finalidad principal del tratamiento. Este patrón permite a los usuarios elegir, de forma desagregada, las funcionalidades del sistema que desean utilizar y proporcionar únicamente los datos requeridos para su consecución. |  | |
| [Control de acceso selectivo](https://www.privacypatterns.org/patterns/Selective-Access-Control) | Utilizado en foros, redes sociales y servicios web de publicación de contenido, proporciona a los usuarios un mecanismo para definir la visibilidad de sus publicaciones y el contenido que comparten mediante la definición de reglas de acceso y la configuración de las opciones de privacidad. |  | |
| [Opción de divulgación selectiva](https://www.privacypatterns.org/patterns/Support-Selective-Disclosure) | Muchos productos y servicios requieren la recopilación de una cantidad prefijada de datos, en ocasiones excesiva, con antelación a que el usuario pueda comenzar a hacer uso de este. Sin embargo, hay personas que prefieren elegir libremente qué tipo de información comparten. Este patrón recomienda que los servicios admitan una opción de divulgación selectiva, adaptando la funcionalidad que se presta al nivel de exposición de datos que el usuario se siente cómodo de compartir. |  |
| [Plataforma de configuración de las preferencias de privacidad](https://privacypatterns.eu/#/patterns/privacy-dashboard/0-0-0-0-0-1-1-0-0-1-0-1-0-0-0-0) | Este patrón permite a los usuarios monitorizar y fácilmente configurar los permisos concedidos y sus preferencias en cuanto a privacidad al ofrecer un punto centralizado donde se puede acceder, previa autenticación, a las opciones configurables que determinan el tratamiento. |  |
| [Control de acceso](http://privacypatterns.wu.ac.at:8080/catalog/) | Establece mecanismos de control de acceso a la información en base al principio de “need to know” para que esta sea procesada legítimamente y por las partes autorizadas. |  |
| [Evaluación de impacto de la privacidad en soluciones de gestión de identidades federadas](https://privacypatterns.eu/#/patterns/federated-privacy-impact-assessment/0-0-0-1-0-0-1-0-0-0-1-0-1-0-0-0) | Las soluciones de gestión de la identidad permiten desacoplar las funciones relacionadas con la autenticación, la autorización y la gestión de los atributos del usuario por un lado y la prestación de los servicios a los que acceden esos usuarios por otro, constituyendo un sistema federado que involucra flujos de datos complejos y la transmisión de la identidad del usuario entre las distintas partes. Estos flujos implican riesgos y amenazas con respecto a la privacidad que deben ser analizados mediante una evaluación de impacto de protección de datos. |  |
| [Gestión de obligaciones](https://privacypatterns.eu/#/patterns/obligation-management/0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0) | El patrón permite que las obligaciones relacionadas con el intercambio, almacenamiento y procesamiento de datos se transfieran y administren entre múltiples partes que intervienen en el tratamiento. De este modo es posible gestionar la política de privacidad definida y las preferencias de usuario, controlando el ejercicio de los derechos o la retirada de consentimientos cuando los datos han sido comunicados o son compartidos por varios responsables/encargados. |  |
| [Auditorías](http://privacypatterns.wu.ac.at:8080/catalog/) | Realizar auditorías periódicas para examinar la efectividad de los mecanismos de cumplimiento. |  |
| [Registro](http://privacypatterns.wu.ac.at:8080/catalog/) | La aplicación de este patrón permite demostrar al responsable en cumplimiento del principio de  accountability que los requisitos normativos en materia de protección de datos están debidamente implantados. |  |
| [Términos y condiciones abreviados](https://privacypatterns.org/patterns/Abridged-Terms-and-Conditions) | Persigue que los usuarios puedan comprender mejor los términos y condiciones presentados en la política de privacidad (riesgos, derechos, cesiones, …) si estos se presentan de una forma concisa y abreviada que sea comprensible para el interesado. |  |
| [Alerta de tratamiento](https://privacypatterns.org/patterns/Ambient-notice) | Proporcionar un aviso discreto, pero claramente perceptible cuando un sensor esté recopilando datos personales o se esté realizando el seguimiento de un individuo de modo que los usuarios puedan obtener más información en tiempo real, si lo requieren, sobre el uso de los datos y así poder revocar los permisos. Una alternativa a este patrón es el denominado Aviso asincrónico |  |
| [Feedback de privacidad](https://privacypatterns.org/patterns/Appropriate-Privacy-Feedback) | Con el objetivo de asegurar que el interesado entiende el alcance del tratamiento se le envía una notificación para confirmar que comprende qué datos son recogidos, a quién se le van a comunicar, cómo van a utilizarse y qué riesgos para su privacidad implica y así pueda ajustar sus preferencias de privacidad antes de utilizar la aplicación o servicio. |  |
| [Iconos de privacidad](https://privacypatterns.eu/#/patterns/privacy-icons/0-1-1-1-0-0-0-1-1-4-0-0-1-0-0-1) | Muchas veces, las políticas de privacidad son enrevesadas y difíciles de entender. El uso de iconos, preferiblemente estandarizados, permite transmitir la información más rápidamente y apoyar la comprensión del texto, convirtiéndose en una herramienta útil para aumentar la trasparencia y el nivel de información que ofrece la política de privacidad. |  |
| [Sensibilización](https://privacypatterns.org/patterns/Awareness-Feed) | Hacer conscientes a los usuarios sobre las potenciales consecuencias de compartir sus datos, informándoles de cuán visibles son y qué riesgos pueden derivarse de esa exposición. Esto les permite reconsiderar sus configuraciones de privacidad y tomar medidas si lo desean. |  |
| [Notificación de brechas de privacidad](https://privacypatterns.eu/#/patterns/data-breach-notification-pattern/0-0-0-0-0-0-0-5-1-0-0-1-0-0-0-0) | Este patrón asegura que no de que, en el caso en que se produzca un acceso y procesamiento no autorizado de datos personales, sea detectado y se informe a la autoridad supervisora y, en su caso, a los usuarios afectados, sin demoras indebidas. |  |
| [Visualización dinámica de la política de privacidad](https://privacypatterns.org/patterns/Dynamic-Privacy-Policy-Display) | No todos los entornos son adecuados para mostrar una política de privacidad extensa y, sin embargo, los interesados necesitan poder consultar información detalladas respecto a algún punto concreto. Este patrón proporciona información adicional de la política de privacidad de manera contextual (haciendo un clic o pasando el ratón por un enlace) ajustada al contexto o dispositivo desde el que se consulta. |  |
| [Gestión y notificación de actividades inusuales en las cuentas de usuario](https://privacypatterns.org/patterns/Unusual-activities) | Muchos servicios web se basan en sistemas de autenticación débiles basados en usuario y contraseña. Conviene establecer mecanismos para identificar actividades anómalas en la cuenta de usuario, alertar a los titulares y utilizar autenticación multifactor para proteger los sistemas de accesos indebidos. |  |
| [Advertencia sobre el grado de divulgación](https://privacypatterns.org/patterns/Impactful-Information-and-Feedback) | Para evitar que los usuarios intercambien o publiquen información de carácter personal de forma inconsciente o por error durante el uso de aplicaciones o servicios pueden utilizarse alertas contextuales de privacidad que ofrezcan información en relación con el nivel de divulgación de los datos antes de que esa información sea definitivamente publicada o transmitida. |  |
| [Contraseñas seguras](https://www.privacypatterns.org/patterns/Informed-Secure-Passwords) | El método habitual de autenticación para acceder a un servicio es en forma de usuario y contraseña. Debido a la debilidad de este método de autenticación el responsable debe utilizar este patrón para asistir al usuario en la elección de una contraseña robusta y mantenerles informados de la importancia de su protección y custodia. |  |
| [Diseño de capas de](https://privacypatterns.eu/#/patterns/layered-policy-design/0-0-0-0-0-0-0-0-0-2-0-0-1-0-0-0)  [políticas de privacidad](https://privacypatterns.eu/#/patterns/layered-policy-design/0-0-0-0-0-0-0-0-0-2-0-0-1-0-0-0) | Las políticas de privacidad tienden a ser largas, complejas y difíciles de entender  lo que lleva a que el usuario no las lea y en consecuencia no esté adecuadamente informado del tratamiento. Este patrón sugiere que el responsable organice la política de privacidad en niveles anidados de detalle y extraiga los aspectos más relevantes a un primer nivel para, desde cada uno de ellos, proporcionar acceso a los sucesivos niveles de detalle donde los usuarios puedan encontrar de una forma fácil y cómoda la información relevante para ellos. |  |
| [Minimización de la asimetría de información](https://www.privacypatterns.org/patterns/Minimal-Information-Asymmetry) | La asimetría de información se define como la situación en la que una de las partes involucrada en una transacción tiene más o mejor información sobre esta que la otra. Para que exista una relación de confianza entre el responsable y el sujeto de datos, este debe conocer y entender la naturaleza del tratamiento. El uso de este patrón se traduce en minimizar la cantidad y tipo de datos obtenidos del usuario para que sólo se procesen los datos personales requeridos para el propósito perseguido y establecer políticas claras y concisas fácilmente comprensibles por el usuario, reduciendo así el desequilibrio responsable – sujeto de datos. |  |
| [Registro de datos personales](https://privacypatterns.org/patterns/Personal-Data-Table) | Aun cuando en muchos casos no constituye una obligación legal para el responsable, la publicación del inventario de tratamientos fomenta la transparencia y haciéndolos fácilmente accesibles por el usuario permite que estos estén informados con todo detalle de las características del tratamiento: qué datos se recogen, por quién, para qué finalidad, a quiénes se comunican, por cuánto tiempo se conservan, … Puede valorarse incluso la posibilidad de dar acceso en bruto al registro de los datos que son objeto de tratamiento a distinto nivel de detalle. |  |
| [Panel de concienciación en](https://www.privacypatterns.org/patterns/Privacy-Awareness-Panel)  [privacidad](https://www.privacypatterns.org/patterns/Privacy-Awareness-Panel) | Existen servicios y aplicaciones que tienen un impacto en la privacidad del usuario de maneras que no resultan evidentes para el usuario en un primer momento. Es posible que los usuarios, si no son plenamente conscientes de las consecuencias y actúan desinformados, tomen decisiones incorrectas en relación con cómo utilizan los servicios pudiendo incluso llegar a pensar que las acciones que realizan son anónimas y no les identifican. Este patrón permite enviar a los usuarios recordatorios sobre quién puede ver el contenido que divulgan, qué se hace con él y cómo podría llegar a identificárseles. |  |
| [Codificación de privacidad mediante colores](https://privacypatterns.eu/#/patterns/privacy-color-coding/0-0-0-0-0-0-0-0-0-0-0-0-1-0-0-0) | Utilizado en entornos web en lo que se publican datos personales, como las redes sociales, permite a los usuarios apreciar rápidamente y a simple vista mediante la codificación por medio de colores cuáles son los parámetros de privacidad que se aplican al contenido compartido. |  |
| [Etiquetas de privacidad](https://www.privacypatterns.org/patterns/Privacy-Labels) | Debido al esfuerzo requerido, los usuarios a menudo no consultan las diversas políticas de privacidad de los servicios que utilizan lo que conduce a desinformación sobre las posibles consecuencias de su consentimiento y opciones de privacidad configuradas. Definir los aspectos básicos del tratamiento de forma tabular y haciendo uso de etiquetas ayuda a comprender más fácilmente la naturaleza y características del tratamiento. |  |
| [Espejos de privacidad](https://www.privacypatterns.org/patterns/Privacy-Mirrors.html) | Los usuarios, con frecuencia, desconocen el nivel al que un sistema procesa sus datos personales. Debido a esto, unas veces se acepta el uso indefinido y sin control de los datos y otras, por el contrario, se limita más de lo necesario resultando en una pérdida de funcionalidad. Este patrón implementa un sistema una reflexión a alto nivel sobre qué datos personales conoce el sistema, qué acceso se le da a otros y qué tipo de datos personales se pueden deducir proporcionando así una interfaz que permite a los usuarios considerar su privacidad en contexto y tomar decisiones informadas ajustadas a sus necesidades. |  |
| [Proxy de privacidad](https://privacypatterns.eu/#/patterns/privacy-aware-network-client/0-0-0-0-0-0-0-2-0-0-0-0-1-0-0-0) | Las políticas de privacidad publicadas en servicios web son, en muchas ocasiones, difíciles de leer y entender por los interesados. Este patrón, aplicable a soluciones web, implementa un proxy de privacidad capaz de analizar e interpretar las políticas y traducirlas a un formato más fácil de leer. |  |
| [Selección de credenciales](https://privacypatterns.org/patterns/Informed-Credential-Selection) | En procesos que requieren autenticación, proporcionar información exacta a los usuarios de los datos personales y los metadatos que el responsable obtendrá una vez finalizada la transacción y habilitar un mecanismo que permita seleccionar entre diferentes opciones, permitiendo identificarse de manera granular, proporcionando más o menos información según su elección. |  |
| [Anonimización](http://privacypatterns.wu.ac.at:8080/catalog/) | Desvincular los atributos sensibles de los identificadores correspondientes para que los sujetos de datos no puedan ser identificados. |  |
| [Seleccionar antes de recoger](http://privacypatterns.wu.ac.at:8080/catalog/) | Su implementación limita la recogida de datos personales a los necesarios para los propósitos especificados y para los que existe una base jurídica, evitando así una recopilación indiscriminada de datos  y potencialmente, un desvío de finalidad del tratamiento. |  |
| [Eliminación de metadatos](https://privacypatterns.eu/#/patterns/strip-metadata/0-0-0-0-0-0-0-0-0-4-0-0-0-0-0-0) | Deben ocultarse los metadatos que se generan durante determinados tratamientos (datos exif en las fotografías, cabeceras en el email o en otro tipo de comunicaciones, sellos de tiempo en los ficheros, … ) que no son necesarios para la finalidad perseguida y que, si se hacen públicos, pueden representar una amenaza para la privacidad. |  |
| [Credenciales basadas en atributos](https://privacypatterns.eu/#/patterns/attribute-based-credentials/0-0-0-0-0-0-0-3-0-0-0-0-0-0-0-0) | Permiten autenticar de manera flexible y selectiva el cumplimiento de diferentes propiedades o atributos sobre una entidad o sujeto, pero sin revelar su identidad o información adicional sobre ella (propiedad de conocimiento cero) |  |
| [Protección frente al seguimiento](https://privacypatterns.eu/#/patterns/protection-against-tracking/0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0) | Este patrón evita el seguimiento de las personas que visitan un sitio web a través del empleo de cookies, mediante la implementación de mecanismos entre el navegador y el servidor web que se encarguen de eliminarlas de forma regular (por ejemplo, en cada inicio del sistema operativo) o deshabilitándolas de manera permanente. |  |
| [Redes de mezcla](http://privacypatterns.wu.ac.at:8080/catalog/) | Las redes de mezcla son protocolos de enrutamiento que crean comunicaciones difíciles de rastrear usando una cadena de servidores proxy que reciben mensajes de múltiples emisores, los reordenan y los reenvían en orden aleatorio al próximo destino (posiblemente otro nodo de mezcla). De esta manera se rompe el enlace entre la fuente de la petición y el destino, haciendo más difícil la tarea de alguien que pretende escuchar las comunicaciones de extremo a extremo. Este patrón proporciona desvinculación en las comunicaciones extremo a extremo dificultando establecer correlaciones y el rastreo de las comunicaciones. |  |
| [Encaminamiento de cebolla](https://privacypatterns.eu/#/patterns/onion-routing/0-0-0-0-0-0-0-0-0-0-0-0-1-0-0-0) | Este patrón es un caso particular del patrón de Redes de mezcla y proporciona desvinculación entre el emisor y el receptor de una comunicación encapsulando los datos en diferentes capas de cifrado y limitando así el conocimiento por parte de los nodos intermedios de la ruta de la comunicación logrando así un enrutado anónimo. |  |
| [Seudonimización](http://privacypatterns.wu.ac.at:8080/catalog/) | Este patrón permite realizar el tratamiento de datos personales de manera que no puedan atribuirse a un sujeto de datos específico sin el uso de información adicional, siempre que dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas para garantizar la no atribución |  |
| [Identidad seudónima](https://www.privacypatterns.org/patterns/Pseudonymous-identity) | Es posible interaccionar de forma anónima en determinados servicios, como los foros, mediante el uso de seudónimos que oculten la identidad real del interesado en sus participaciones, de modo que el resto de los usuarios no puedan vincularlas con la identidad real del sujeto. |  |
| [Mensajería seudónima](https://privacypatterns.eu/#/patterns/pseudonymous-messaging/0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0) | Se trata de un servicio de mensajería en línea mejorados en el que un tercero de confianza se encarga de intercambiar los identificadores de las partes involucradas en la comunicación por seudónimos manteniendo así la anonimidad entre los extremos. |  |
| [Enmascaramiento](https://privacypatterns.eu/#/patterns/use-of-dummies/0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0) | Este patrón oculta las acciones realizadas por un usuario al agregar otras interacciones falsas que no se pueden distinguirse de las reales. Se utiliza para proteger la privacidad en servicios de localización notificando diferentes ubicaciones para ocultar la localización real, en comunicaciones anónimas mediante el envío de mensajes falsos a destinatarios falsos para proteger el perfil, o en servicios de búsqueda web para ocultar las preferencias reales. |  |
| [Conjunto anónimo](https://privacypatterns.org/patterns/Anonymity-set) | Agrega múltiples ocurrencias de registros relativos a interesados en un único conjunto de datos, de modo que no se pueda identificar una ocurrencia concreta dentro del conjunto, evitando así acciones como realizar seguimiento de la localización de un sujeto, analizar el comportamiento u otras operaciones que pueden poner en riesgo la privacidad |  |
| [Cifrado con claves administradas por el usuario](https://privacypatterns.org/patterns/Encryption-user-managed-keys) | Protege la confidencialidad de la información personal codificando el contenido de los mensajes transmitidos por la red o almacenados usando un servicio proporcionado por terceros no confiables mediante el uso de algoritmos de cifrado y utilizando claves administradas por el usuario, de modo que sólo aquellos que dispongan de la clave de descifrado pueden recuperar el contenido |  |
| [Bloqueo de correlación en sistemas de gestión de identidad federada](https://privacypatterns.eu/#/patterns/identity-federation-do-not-track-pattern/0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0) | En sistemas de gestión de identidad federada el uso de este patrón evita la correlación de las solicitudes entre el usuario final y el proveedor de los servicios que pueden llegar a hacer los otros actores participantes en el sistema mediante el uso de un orquestador de las peticiones que corre en el entorno cliente. |  |
| [Custodia de datos por el usuario](https://privacypatterns.eu/#/patterns/user-data-confinement-pattern/0-0-2-0-0-0-0-0-1-0-0-0-0-0-0-1) | Es habitual desarrollar arquitecturas de tipo centralizado en las que el tratamiento de los datos personales se realiza en un único sistema o entidad en el que el usuario se ve obligado a confiar e incluso compartir datos sensibles. Este patrón evita un tratamiento centralizado de los datos personales al trasladar parte de este a entornos de confianza del usuario (por ejemplo, sus propios dispositivos), permitiéndoles así controlar los datos exactos que son compartidos con los proveedores de servicios. |  |
| [Listas negras anónimas](https://privacypatterns.eu/#/patterns/anonymous-reputation-based-blacklisting/0-1-0-5-2-0-2-3-1-0-0-1-0-1-0-0) | Mantener el control sobre los usuarios que hacen un uso incorrecto del servicio y prohibirles el acceso creando listas negras, pero sin conocer su identidad. |  |

## XII. BIBLIOGRAFÍA

* 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) [https://eur-lex.europa.eu/legal-](https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&qid=1592307014433&from=ES)

[content/ES/TXT/HTML/?uri=CELEX:32016R0679&qid=1592307014433&from=ES](https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&qid=1592307014433&from=ES)

* Guidelines 4/2019 on Article 25 Data Protection by Design and by Default [https://edpb.europa.eu/our-work-tools/public-consultations-art-](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_es)

[704/2019/guidelines-42019-article-25-data-protection-design\_es](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_es)

* “Recommendations on shaping technology according to GDPR provisions. Exploring the notion of data protection by default”, dic 2018. European Union Agency for Cybersecurity (ENISA).

[https://www.enisa.europa.eu/publications/recommendations-on-shapingtechnology-according-to-gdpr-provisions-part-2](https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2)

Página: 39 de 39