Orientaciones para la validación de sistemas criptográficos en la protección de datos

v. mayo de 2023

RESUMEN EJECUTIVO

El uso generalizado de los servicios y las tecnologías de la información y comunicación ha hecho que el cifrado sea una de las medidas más importantes para proteger la seguridad de los datos. Los mecanismos criptográficos, adecuadamente implementados, proporcionan medidas robustas de protección de los datos personales en tratamientos automatizados a la hora de asegurar confidencialidad, integridad y autenticidad.

La fortaleza y robustez de un sistema de cifrado, esto es, su capacidad para resistir ataques destinados a romper la protección que proporciona depende de su comportamiento como sistema, no exclusivamente de cada componente de forma independiente. Para poder ofrecer un nivel adecuado de protección, los sistemas de cifrado han de ser eficaces y efectivos en el marco de cada tratamiento concreto, además de ser operativos.

El RGPD menciona explícitamente el cifrado como una medida para la mitigación de riesgos de seguridad en la protección de datos personales para:

- asegurar un nivel de seguridad apropiado para el riesgo a los derechos y libertades de los titulares de datos personales,
- garantía que forma parte de las condiciones para la conformidad con el RGPD,
- como salvaguarda que disminuye la probabilidad de un impacto sobre los interesados en el marco de una brecha de datos personales.

Por lo tanto, como medida de protección, el cifrado no tendrá el mismo impacto en todos los tratamientos, y necesariamente estará complementado por otras garantías de privacidad y medidas de seguridad.

Para que el cifrado sea una medida efectiva en un tratamiento, el responsable, o el encargado, ha de verificar, evaluar y valorar todos los elementos que intervienen en el proceso de cifrado, más allá de limitarse a la selección de un algoritmo o una implementación concreta de éste. Por un lado, hay que determinar los requisitos que ha de cumplir el sistema de cifrado en el contexto del tratamiento, y por el otro ha de realizarse una validación de que dichos requisitos se satisfacen, así como supervisar que se mantienen en el tiempo. En todo caso hay que tener en cuenta que la protección de datos personales implica considerar el tiempo de vida de dichos datos, que puede ser tan extenso como la vida del titular de los datos y ello en el contexto de los cambios tecnológicos que ocurren en largos lapsos de tiempo. Es importante resaltar que el cifrado no comporta anonimización, aunque podría utilizarse como herramienta de seudonimización.

En estas orientaciones se desgranan los elementos que es recomendable evaluar en el diseño y validación de un sistema de cifrado empleado en un tratamiento de datos personales teniendo en cuenta la transcendencia de este en dicho tratamiento, y especialmente centrado en aquellos casos en el que el cifrado se emplea para preservar la confidencialidad. Además, se propone una lista de controles, no exhaustiva ni exigible en su totalidad, para facilitar al responsable o encargado RGPD del tratamiento, al responsable funcional dentro de estas entidades, al DPD, a los asesores en protección de datos y a auditores internos y externos, la selección, validación y supervisión de los sistemas de cifrado en el marco de un tratamiento específico, como parte de las labores de privacidad desde el diseño y responsabilidad proactiva.

Palabras clave: criptografía, cifrado, claves, algoritmo, mitigación, riesgo, RGPD, auditoría, protección de datos.

El presente documento ha sido desarrollado por la Agencia Española de Protección de Datos en colaboración con la Asociación Profesional Española de Privacidad (APEP) y la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum) y las revisiones realizadas por Carlos Bachmaier, DPD de Sociedad Estatal, María Isabel González Vasco, Catedrática del Departamento de Matemática Aplicada, Ciencia e Ingeniería de los Materiales y Tecnología Electrónica (MACIMTE) de la Universidad Rey Juan Carlos e Isabel Barberá, Ingeniera de Privacidad de Rhite.

ÍNDICE

1 INTRODUCCIÓN

El cifrado es un procedimiento por el cual una información (que se denominará información en claro) se transforma en un conjunto aparentemente ininteligible de datos (o información cifrada). Para conseguir este objetivo, la criptografía actual conjuga transformaciones basadas en algoritmos matemáticos, implementaciones "seguras" de los mismos y el uso de claves. El aspecto característico del cifrado es que, sin acceso a la clave adecuada, debería resultar inviable (al menos en un marco temporal y de recursos) acceder al contenido de la información cifrada, o alterar la misma sin que los cambios fueran detectados.

El cifrado como medida aparece explícitamente en el 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 o RGPD), y en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (LO 7/2021). En el RGPD aparece entre las medidas que es posible aplicar para la mitigación de riesgos de seguridad en la protección de datos personales (Considerando 83 y Artículo 32), como salvaguarda que coadyuva para establecer la compatibilidad del tratamiento (Artículo 6 apartado 4) o como salvaguarda que disminuye la probabilidad de un impacto para los interesados en el marco de una brecha de datos personales y hace potestativa la comunicación a los interesados (Artículo 34).

El cifrado es una medida adecuada de seguridad siempre que su implementación, así como su operación, se ajuste a las características y al impacto del tratamiento. En caso contrario, se convierte en una medida que genera una sensación de falsa seguridad que relaja la aplicación de otras medidas complementarias en el tratamiento, en particular, garantías de privacidad desde el diseño.

Limitar la cuestión del cifrado a la mera selección de un algoritmo es una visión simplista que deja de lado aspectos esenciales que pueden hacer inútil dicha medida. Un sistema de cifrado o criptosistema es mucho más complejo, y se puede entender como todos los elementos que conforman los procesos de cifrado y descifrado enmarcados en el tratamiento de datos personales: el algoritmo, su implementación, la creación y la gestión del ciclo de vida de las claves, las herramientas que conforman su suite, la comunicación, los dispositivos empleados, el modelo de gobernanza, etc. La aplicación del principio de responsabilidad proactiva (art. 5.2 y art. 24.1 del RGPD) hace precisa una validación[1] del sistema criptográfico en los tratamientos de datos personales en el marco de la naturaleza, el ámbito o alcance, el contexto y los fines específicos de cada tratamiento..

En nivel de detalle en el diseño, la validación y la supervisión del sistema criptográfico ha de adecuarse a la importancia y relevancia que tiene el cifrado en el tratamiento de los datos, así como el impacto que tiene dicho tratamiento para los derechos y libertades de los interesados.

El papel del cifrado en un tratamiento podría ser el de una salvaguarda adicional entre las muchas que se encuentran implementadas en un tratamiento concreto, o incluso una medida

[1] El acto documentado de probar que cualquier procedimiento, proceso, equipo, material, actividad, o sistema conduce realmente a los resultados esperados. Proceso de confirmar que un elemento (un sistema, un producto de trabajo o una parte del mismo) coincide con las necesidades de sus partes interesadas.

de protección de datos por defecto[2]. También podría ser el de una medida determinante en un tratamiento para gestionar un alto riesgo o incluso ser el de una de las medidas sobre las que se fundamenta que existen garantías suficientes para proteger los derechos de los interesados. En este último caso, podríamos hacer referencia a distintos artículos del RGPD en los que las medidas son una parte importante para determinar la conformidad con los requisitos de la normativa de protección de datos:

- Ponderación del interés legítimo (art. 6.1.f)
- Determinación de tratamientos compatibles (art. 6.4.e)
- Las limitaciones a los derechos establecidos por ley (art. 23)
- La elección de un encargado de tratamiento (art. 28)
- La reducción de un alto riesgo del tratamiento (art. 32) y (art. 33.7.d)
- La no comunicación de una brecha de datos personales a los interesados. (art. 34.3.a)
- La superación de la evaluación de la proporcionalidad del tratamiento (art. 35.7.b)
- Los códigos de conducta y certificación (art. 40, 41 y 42)
- La conformidad con el RGPD de transferencias internacionales de datos (art. 46, 47, 49 y 50)
- El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos (art. 89)

La fortaleza de un sistema de cifrado es una estimación, de forma objetiva, de la posibilidad de que sea comprometido en un periodo dado de tiempo. Esta posibilidad debería ser muy baja, en el caso de protección de datos, durante todo el tiempo de vida de dicho dato personal. Dicha fortaleza no depende exclusivamente del algoritmo empleado ni de la longitud de la clave, y no todos los sistemas tienen la misma fortaleza. Utilizar un sistema de cifrado muy fuerte puede suponer un elevado coste, tanto en la implementación como en la operación del tratamiento, y, además, entrar en conflicto con el cumplimiento de otros requisitos (ajenos a la protección de datos) que el mismo tratamiento precisa en relación con la latencia, tiempo de establecimiento, consumo, recursos, rendimiento, portabilidad, usabilidad, coste, retorno de la inversión en seguridad, etc.

Sin embargo, desde el punto del RGPD, rebajar los niveles de seguridad por debajo de los adecuados, poniendo en riesgo los derechos y libertades de los interesados, atendiendo a criterios distintos de la protección para los derechos y libertades no es aceptable.

En particular, en el caso de que la garantía principal sobre la que descansa un tratamiento sea el cifrado de los datos personales, es necesario realizar la validación exhaustiva de la fortaleza del criptosistema[3]. Esta validación ha de realizarse "desde el diseño" y el empleo del sistema de cifrado ha de estar integrado en el tratamiento tal y como se establece en la Guía de Privacidad desde el Diseño publicada por la AEPD.

En cualquier caso, las políticas de protección de datos personales, que formarían parte del marco de gobernanza o política de información de la entidad, a las que se refiere el artículo 24 del RGPD, deberán reflejar las estrategias del responsable con relación a los sistemas criptográficos desde la perspectiva de protección de datos, e integrarse en los procedimientos de gestión de la seguridad de los sistemas de información.

---

[2] El artículo 25 reclama el establecimiento de medidas técnicas y organizativas apropiadas para gestionar tanto para "los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas" así como en función de "la naturaleza, ámbito, contexto y fines del tratamiento" aunque no exista riesgo para los derechos y libertades de los interesados.

[3] OWASP ha establecido los fallos en el sistema de cifrado como el segundo factor más importante de riesgo de seguridad en la web en 2021

Estas orientaciones no llegan al detalle de todos los casos específicos de implementaciones concretas, ni aborda una parte importante como la asignación de roles en todo el proceso, sino que son un punto de partida para que los destinatarios de este documento tengan un marco inicial de análisis y, según su criterio, seleccionen las comprobaciones que estimen pertinentes y añadan aquellas que resulten adecuadas para la especificidad del tratamiento.

2 CONSIDERACIONES INICIALES

2.1 DESTINATARIOS

Estas orientaciones están dirigidas a los responsables y encargados/subencargados de tratamientos a los que se les aplique el RGPD o la LO 7/2021, que aplican criptografía en sus tratamientos de datos personales. Por lo tanto, también está orientada a los delegados de protección de datos, a los asesores en materia de protección de datos personales, a los auditores de protección de datos, a los especialistas en seguridad, y responsables funcionales[4] de las entidades responsables o encargadas. También se aconseja esta guía a desarrolladores de soluciones de cifrado que estén destinadas al tratamiento de datos personales y, en general, a los desarrolladores de productos y servicios de los sistemas TIC.

2.2 OBLIGACIONES

El responsable y los posibles encargados/subencargados del tratamiento (art. 32.1 del RGPD) tienen la obligación de que las medidas de seguridad implementadas con el objeto de gestionar los riesgos para los derechos y libertades sean eficaces y sean sometidas a un proceso de verificación, evaluación y valoración regulares (art. 32.1.d).

Hay que subrayar que las medidas establecidas en el marco del artículo 32 han de evaluarse de forma regular, a diferencia del resto de medidas técnicas y organizativas apropiadas, a fin de garantizar y poder demostrar que el tratamiento es conforme con el artículo 24.1 del RGPD que establece que tendrán que revisarse y actualizarse cuando sea necesario.

La implementación práctica de un tratamiento (lo que define la naturaleza del tratamiento) implicará la adquisición de componentes, el uso de servicios, posiblemente la contratación de encargados, subencargados y la comunicación de datos, lo que afectará también al criptosistema como parte de las medidas de seguridad.

El responsable del tratamiento tiene que definir el reparto de obligaciones en la gestión de la seguridad con los encargados, en particular con relación al sistema de cifrado, teniendo en cuenta que, normalmente, parte de la gestión directa quedará en sus manos. Para el caso de componentes y uso de servicios de terceros para la implementación del criptosistema, los responsables y encargados/subencargados tendrán que ser diligentes a la hora de requerir las certificaciones de eficacia ajustadas a los requisitos del tratamiento concreto y la normativa en vigor.

2.3 EL PAPEL DEL DPD

En aquellos casos en los que esté designado un DPD, éste tiene, entre otras funciones, la de informar y asesorar al responsable o al encargado del tratamiento, y a los empleados de los mismos, de las obligaciones derivadas del RGPD (art. 39.1.a), la de supervisar el cumplimiento de la normativa de protección de datos, la concienciación y formación del personal, las auditorías, (art. 39.1.b) y, en caso de una Evaluación de Impacto para la Protección de Datos, asesorar y supervisar su aplicación (art. 39.1.e).

Esta misión de asesoramiento y supervisión se podría materializar en las auditorías generales de protección de datos y las auditorías regulares con relación a la correcta aplicación de las medidas de seguridad. En particular, el DPD ha de estar informado de

[4] No hay que confundir la figura de responsable RGPD-L.O. 7/2021 de un tratamiento, figura legal definida en los arts. 4.7 RGPD y 5.g LO 7/2021, que generalmente corresponde a una persona jurídica, con la figura de "responsable" de una tarea asignada a una persona física u órgano en el marco de la organización de una entidad. Puede recibir la designación de responsable del proceso, del sistema de información, encargado funcional, "data owner", "risk owner". En esta guía se designará como responsable funcional

cualquier tipo de incidente interno y de los cambios de contexto con relación al sistema de cifrado. El DPD, con dicha información y atendiendo las características del tratamiento como un todo, podrá elevar sus conclusiones y recomendaciones a los órganos máximos de dirección de responsables y encargados.

Con relación al objeto de estas orientaciones, el DPD ha de conocer el tratamiento y qué requisitos se derivan para el/los criptosistemas que se implementarán en el mismo. Tendrá que asesorar y, dentro de sus funciones de supervisión del cumplimiento con lo dispuesto en el RGPD, supervisar el proceso regular de verificación, evaluación y valoración del funcionamiento apropiado del sistema de cifrado.

En definitiva, el DPD deberá:

- Conocer la naturaleza o cómo está implementado el tratamiento.
- Conocer el nivel de riesgo para los derechos y libertades de dicho tratamiento.
- Conocer qué trascendencia tiene el criptosistema en el conjunto de medidas de seguridad que determinan la viabilidad del tratamiento desde el punto de vista de los derechos y libertades.
- Asesorar sobre los requisitos que se derivan para el sistema/s de cifrado, qué elementos del mismo son más críticos y qué comprobaciones deberían llevarse a cabo.
- Supervisar el proceso regular de verificación, evaluación y valoración de los controles.
- Informar a la dirección de la organización.

Dentro de un proceso de mejora continua, la auditoría es una de las mejores herramientas de gestión que puede ser utilizada por el DPD para definir las recomendaciones que transmitirá al responsable del tratamiento y para asegurar la fortaleza del criptosistema con relación a la protección de datos personales.

También es buena práctica supervisar con regularidad cómo los encargados/subencargados y los proveedores de las organizaciones mantienen su sistema de cifrado, empezando, por ejemplo, con un '*vendor assessment*'[5].

2.4 MÁS ALLÁ DE LA CONFIDENCIALIDAD

El sistema de cifrado puede emplearse tanto para proteger la confidencialidad del dato personal, como para determinar la integridad de la información, así como en los procesos de autenticación, no repudio y seudonimización.

Aunque este documento se centra en el cifrado como medida para preservar la confidencialidad, podrá ser de ayuda cuando en el tratamiento se empleen sistemas de cifrado con los propósitos anteriormente señalados, y cuando el fallo de dichas medidas pudiera afectar a los derechos fundamentales con relación a la protección de datos.

2.5 SEGURIDAD DESDE EL DISEÑO Y VALIDACIÓN

El responsable del tratamiento, antes de incluir un sistema de cifrado en el tratamiento, ha de llevar a cabo dos tareas:

- Determinar desde el diseño los requisitos de fortaleza del criptosistema que son necesarios en el tratamiento y
- Validar que dichos requisitos se están alcanzado de forma efectiva en la implementación de los sistemas de información y en su operativa.

[5] Proceso de evaluación y aprobación de proveedores potenciales mediante una evaluación objetiva.

El art. 24.1 del RGPD establece que el responsable aplicará en el tratamiento medidas técnicas y organizativas apropiadas. Las medidas, para ser apropiadas, han de establecerse en función de, por un lado, la naturaleza, contexto, ámbito y fines[6] del tratamiento, y por otro el riesgo que para los derechos y libertades fundamentales de las personas supone el mismo tratamiento. Con relación al riesgo para los derechos fundamentales y a la seguridad, el art. 32 establece que las medidas establecidas han de ser apropiadas para garantizar un nivel de seguridad adecuado. Como ya ha establecido el Tribunal Supremo, las medidas de seguridad son una obligación de medios, no de resultado[7]. Las medidas han de tener tres objetivos: primero asegurar la protección de los derechos y libertades; segundo, el cumplimiento con la normativa; y tercero, poder demostrarlo. Además, la protección y el cumplimiento no son acciones puntuales, sino que exige revisión y actualización, en caso de las medidas de seguridad, de forma regular.

Los requisitos establecidos en el párrafo anterior (garantizar, demostrar y adecuación de las medidas) exigen establecer desde el diseño los requisitos de fortaleza y robustez del criptosistema que son necesarios en el tratamiento. Los requisitos de fortaleza y robustez han de ser establecidos de forma objetiva y han de ser proporcionales al potencial impacto del tratamiento y, en este caso, de la importancia del sistema de cifrado dentro del conjunto de medidas de seguridad en dicho tratamiento. Por ello, se proponen en estas orientaciones cuatro escenarios a la hora de auditar un sistema criptográfico en función del papel que asume la criptografía en el tratamiento. Escenarios que, ordenados de menor a mayor demanda de protección, serían:

- El sistema de cifrado es una medida de protección de datos por defecto.
- El sistema de cifrado es una medida que gestiona riesgos medios y bajos en el tratamiento.
- El sistema de cifrado es una medida que, de forma complementaria, gestiona el alto riesgo para los derechos y libertades en tratamientos.
- El sistema de cifrado es la medida principal o con más peso para gestionar un alto riesgo para los derechos y libertades en el tratamiento, o bien legitimar el tratamiento.

Por otro lado, tanto el art. 24 como el art. 32 del RGPD obligan al responsable a una evaluación y revisión periódicas objetivas. Un instrumento para la revisión y actualización de las medidas es la auditoría, donde se habría de validar la eficacia de las políticas, procedimientos y medidas técnicas y organizativas. Una auditoría del sistema de cifrado, su configuración, implementación y uso, realizada desde la óptica de protección de datos, podrá ser una parte de una auditoría más general de protección de datos del tratamiento.

Un sistema de cifrado que no se evalúa, verifica y valida regularmente en el contexto del tratamiento, es un sistema que no ofrece garantías objetivas. Nótese que una validación, o una auditoría, no es un proceso de "ingeniería inversa[8]". Es decir, el sistema ha de ser diseñado e implementado de forma *accountable*[9] o en aplicación del principio de responsabilidad proactiva[10] (Art. 5.2 del RGPD), lo que implica que se ha utilizado una metodología de desarrollo objetiva, guiada por unos requisitos concretos, con procesos de

---

[6] Por lo tanto, se han de establecer medidas "por defecto", independientemente del riesgo del tratamiento.

[7] Comunicación Poder Judicial: El Tribunal Supremo establece que la obligación de las empresas de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado.

[8] Proceso o método a través del cual uno intenta comprender a través del razonamiento deductivo cómo un dispositivo, proceso, sistema o pieza de software creado previamente realiza una tarea con muy poca idea de cómo lo hace exactamente (si es que hay alguna).

[9] Aunque en el RGPD se ha traducido el término "accountability" por el de responsabilidad proactiva, también utilizaremos el término en inglés por tener una extensión semántica más precisa.

[10] Un tratamiento no puede cumplir el principio de responsabilidad proactiva si las partes que lo componen, o los medios con que se implementa, no lo cumplen.

verificación y validación, y se ha documentado. La comprobación del cumplimiento del principio de responsabilidad proactiva es el primer paso del proceso de validación y/o auditoría. La validación o la auditoría no reemplazan la obligación de responsabilidad proactiva, sino que la complementan.

2.6 REQUISITOS Y TIEMPO DE VIDA DEL DATO PERSONAL

Cada tratamiento tendrá unos requisitos particulares en relación con el sistema de cifrado (latencia, limitaciones en memoria, rendimiento, recursos HW/SW[11], consumo, coste, etc.), además de los requisitos de fortaleza y robustez. Todos ellos están relacionados entre sí, p.ej. una menor latencia requerirá seguramente un mayor consumo y tal vez incrementará el coste. De igual forma, una mayor fortaleza dependerá y repercutirá en el resto de los requisitos.

Los requisitos de fortaleza (seguridad algorítmica y tamaño de la clave) y robustez (seguridad de implementación y operativa) del sistema de cifrado difieren de unas aplicaciones a otras: unas aplicaciones requerirán desde simplemente asegurar la confidencialidad por unos pocos días frente a adversarios poco sofisticados mientras que otras requerirán , hasta la necesidad de proteger la confidencialidad frente a entidades no autorizadas sofisticadas por años, como en el caso de los secretos comerciales e industriales o información con gran impacto individual o social. El tipo de vida del dato, entendido como el periodo de tiempo en que es relevante mantener el mensaje confidencial (o íntegro) es el criterio relevante para determinar los requisitos de fortaleza y robustez del criptosistema.

En el caso de que se utilicen técnicas de cifrado para añadir medidas de seguridad adicionales al tratamiento de datos personales hay que tener presente tanto el impacto que pueda tener la divulgación del dato como cuál es el tiempo de vida del dato desde el punto de vista del RGPD, es decir, el tiempo de vida del dato[12]. Como define el RGPD en el artículo 4.1, un dato personal tiene dicha naturaleza mientras sea información sobre una persona física[13] identificada o identificable.

Si el cifrado va a ser la medida de protección determinante para procesar, almacenar o transmitir información cuya revelación pueda suponer un alto riesgo para los derechos y libertades fundamentales (geolocalización de menores, información sobre víctimas de violencia de género, historias clínicas, hábitos de personas vulnerables o íntimos, perfil o información financiera de gran parte de los sujetos de un país, etc.) estaríamos hablando de requisitos de fortaleza y robustez que ofrezcan una protección razonable por muchos años[14].

2.7 INFORMACIÓN CIFRADA COMO DATO PERSONAL

El uso de cifrado es una de las medidas de protección que se pueden incorporar a un tratamiento de datos personales y podría ser una herramienta adecuada de seudonimización. Sin embargo, hay que tener presente que el hecho de cifrar los datos no

---

[11] Hardware/Software

[12] En el párrafo 84.3 y la nota 70 de las Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE Versión 2.0 se establece "3.la fuerza del cifrado y la longitud de la clave tienen en cuenta el período específico durante el cual debe preservarse la confidencialidad de los datos personales cifrados. Nota: las autoridades públicas pueden comprometerse a acceder a los datos cifrados en las circunstancias descritas en el apartado n.º 80, y almacenarlos hasta que sus recursos sean suficientes para el descifrado. La medida complementaria solo puede considerarse eficaz si ese descifrado y el tratamiento ulterior en ese momento ya no constituyen una violación de los derechos de los interesados, por ejemplo, porque los datos ya no pueden utilizarse para identificarlos directa o indirectamente."

[13] El Dictamen 4/2007 sobre el concepto de datos personales del Grupo de Trabajo del artículo 29, expone que "En principio, la información relativa a personas fallecidas no se debe considerar como datos personales sujetos a las normas de la Directiva, ya que los difuntos dejan de ser personas físicas para el Derecho civil."

[14] A la fecha habría que plantearse si exigirles que fueran cuanto-resistentes, esto es, capaces de soportar ataques de descifrado empleando ordenadores cuánticos de gran potencia.

elimina su naturaleza de dato de carácter personal, por lo que la información cifrada no es información anonimizada[15]. La supuesta "pérdida" o eliminación de una clave de descifrado no cambiará esta naturaleza[16].

2.8 ATAQUES SNLD

En relación con los dos apartados anteriores, el incremento de las capacidades de almacenamiento y tratamiento digital ha puesto sobre la mesa la necesidad de plantearse los futuros ataques SNLD, acrónimo de "Store Now, Decrypt Later" o "almacena ahora y descifra después", también conocidos como HNLD[17].

Actualmente, es posible disponer de ingentes capacidades de almacenamiento de datos por largo tiempo. Esto hace posible la recogida de datos cifrados y mantenerlos a la espera de poder desvelar la información (o el momento adecuado para aplicar recursos para hacerlo). Además, los avances tecnológicos, especialmente con relación a la computación cuántica[18], evidencia la debilidad de los sistemas de cifrado de uso común en un futuro cercano[19] [20].

El impacto que podría tener en el futuro la materialización de estos ataques, tanto para la privacidad de los individuos como la sociedad en su conjunto, ha de evaluarse[21]. Esta evaluación ha de ser especialmente cuidadosa en aquellos casos en los que ingentes cantidades de datos personales bajo la responsabilidad de las Administraciones Públicas se alojan en servicios externos que están protegidos, en tránsito o en su almacenamiento, por medios de cifrado.

2.9 LA CLAVE COMO DATO PERSONAL

La clave de una persona física es un identificador único y su empleo permite identificar a la persona que la usa, y en estas condiciones, por tanto, se trata de un dato de carácter personal en el marco de tratamientos específicos.

2.10 INFORMACIÓN CIFRADA: EN REPOSO, EN TRÁNSITO Y EN CÓMPUTO

Simplificando, hay dos aproximaciones que se podrían considerar como los casos tipo de criptosistemas:

- El cifrado en datos en reposo: los datos se cifran para su almacenamiento protegido frente a pérdida de confidencialidad.
- En tránsito: los datos se cifran previamente a su remisión a un destinatario, bien por redes o utilizando otro tipo de soportes. El destinatario puede o no disponer de los medios para su descifrado, como puede ocurrir para un almacenamiento cifrado en la

---

[15] En un análisis formal basado en la Teoría de la Información, la anonimización supone pérdida de información, mientras que un conjunto de datos cifrado no supone pérdida de información.

[16] Para que la eliminación de la clave supusiera anonimidad tendríamos que encontrarnos con un criptosistema de secreto perfecto, en el que se preservase la distancia de unicidad, el límite del cumpleaños, la entropía de mensajes y claves tendiese a infinito, las implementaciones (programas, librerías, sistemas operativos y dispositivos) no tuvieran fisuras, la gestión y políticas perfectas, las personas perfectas, los algoritmos perfectos y resistentes a ataques de cualquier tipo durante más de 50 años (datos personales son personales durante la vida de las personas), etc. Es decir, estaríamos exigiendo una obligación de resultado, no de medios como ha establecido el TS y por tanto no exigible jurídicamente. Incluso si se pudiera garantizar, estaríamos hablando de casos singulares, no de la operativa común de cifrados masivos de datos.

[17] H de "harvest" o cosechar, aunque también se interpreta SNLD como Steal now, decrypt later.

[18] Aunque no es necesaria la computación cuántica para materializar dichos ataques: https://dl.acm.org/doi/pdf/10.1145/3560107.3560182

[19] https://newsroom.ibm.com/2023-02-23-IBM,-Vodafone,-Other-GSMA-Taskforce-Members-Outline-Critical-Pathways-to-Protect-Telcos-Against-Quantum-Era-Cyberthreats

[20] https://cacm.acm.org/news/269080-nist-post-quantum-cryptography-candidate-cracked/fulltext

[21] https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf

nube. Los datos se pueden cifrar bien para protegerlos durante la transmisión, bien para su almacenado remoto de forma cifrada.

- En cómputo: los datos se generan cifrados o se cifran, siendo tratados, posteriormente, siempre sin descifrar, descifrando únicamente el resultado cuando es necesario.

Este último caso está en diversos grados de sustanciación y es la frontera del estado del arte del cifrado, por lo que se tratará en este documento de los dos primeros casos. El proceso del cifrado de información en reposo, a grandes rasgos, podría considerarse formado por estos grandes bloques:

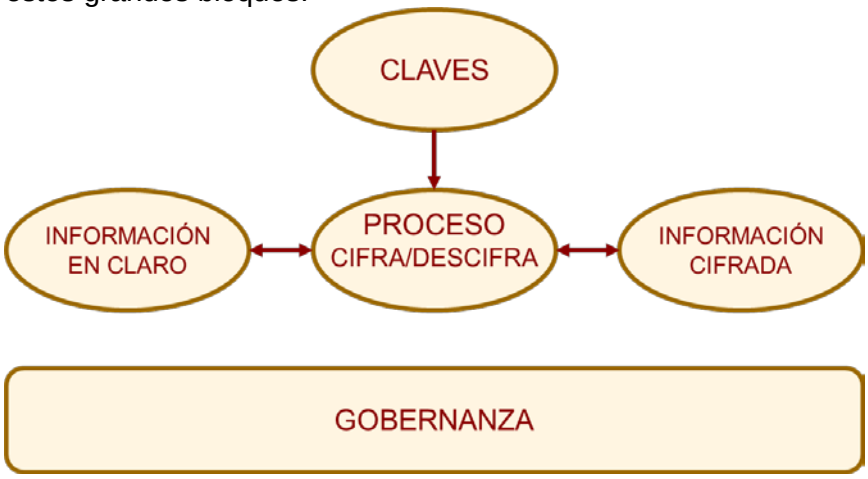


Figura 1 Cifrado de datos en reposo

En caso de estar orientado a la transmisión confidencial de información, existen nuevos elementos que hay que tener en consideración, como el establecimiento de claves con un receptor y la comunicación de mensajes, además de una réplica de todos los elementos del emisor en el receptor (que solo se insinúan en la figura adjunta):

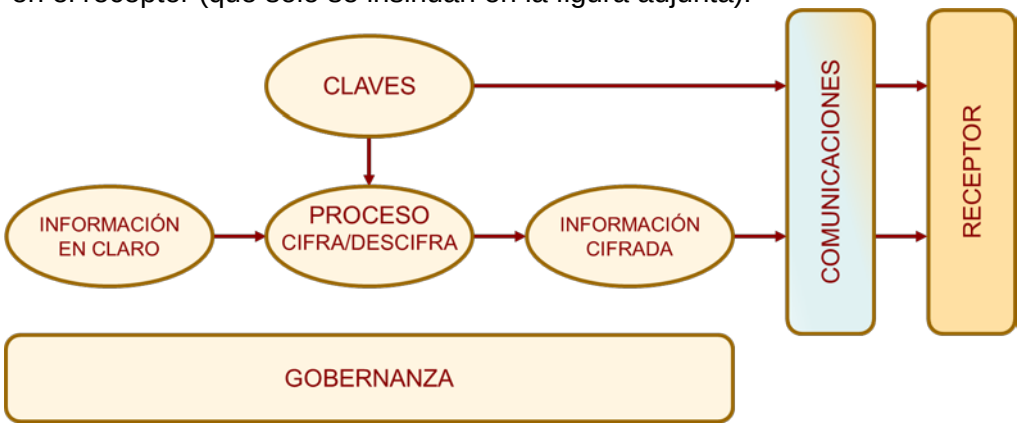


Figura 2Cifrado de datos en transmisión

En el caso de cifrado para transmisión, asegurar la autenticidad y la integridad del mensaje suelen ser requisitos imprescindibles.

Los casos de uso tipo aquí presentados son casos básicos con propósitos didácticos. En los tratamientos prácticos podemos encontrar una combinación de varios procesos o la aplicación de distintos sistemas de cifrado en algunas fases de un mismo tratamiento. Por ejemplo, en un servicio de almacenamiento en la Nube, en que los datos se transmiten a la Nube por un canal asegurado mediante cifrado y, además, los datos están en sí mismo cifrados en origen o son cifrados en reposo por el servicio de la Nube.

Algunos tratamientos específicos pueden mostrar una gran complejidad en la aplicación de sistemas de cifrado, como son los sistemas de mensajería en entornos asíncronos[22], cifrado polimórfico, re-cifrado proxy, cifrado de elementos multimedia, etc.

Esta orientación servirá como punto de partida y tendrá que adaptarse a las peculiaridades de cada sistema, teniendo en cuenta que este es un campo en pleno desarrollo, con algunas aplicaciones disponibles usando tecnologías PET y PEC.

2.11 PRIVACY ENHANCING CRYPTOGRAPHY

Las PET o Privacy Enhancing Technologies son aquellos productos y servicios desarrollados específicamente para facilitar la implementación de medidas de privacidad en los tratamientos. Un subconjunto de ellas son la PEC o Privacy Enhancing Cryptography.

Con relación a las PEC, la oficina de Estándares y Tecnología de EEUU (NIST) señala una serie de herramientas criptográficas avanzadas especialmente adecuadas para implementar estrategias de privacidad desde el diseño:

- Pruebas de Conocimiento Cero (ZKPoK)
- Computación Segura Multiparte
- Cifrado Homomórfico
- Firmas de Grupo y de Anillo
- Protocolos de Intersección Privada (PSI)
- Protocolos de Acceso a Información Privada (PIR)
- Cifrado estructurado (StE)
- Searchable Symmetric Encryption (SSE)

A través de estas herramientas, es posible implementar soluciones avanzadas adecuadas a diferentes escenarios y casos de uso, como, por ejemplo:

- Gestión de credenciales para acceso a servicios con garantías de anonimato.
- Gestión de bases de datos cifradas y compartidas, con distintos niveles de acceso.
- Diseño de métodos de análisis de datos y aprendizaje automático sobre datos cifrados.
- Verificación y auditoría con garantías de privacidad en distintos entornos.

2.12 DOCUMENTACIÓN DE LOS REQUISITOS DEL SISTEMA DE CIFRADO

El responsable del tratamiento debe determinar desde el diseño los requisitos de los sistemas de cifrado, y dichos requisitos han de estar guiados por la gestión de riesgo, al menos, del riesgo para los derechos y libertades de los interesados. En su elaboración, puede resultarle conveniente emplear la clasificación presentada en el punto siguiente, de tal forma que, además de disponer de una guía para la creación de los mismos, se hará más eficaz el proceso de verificación, evaluación y valoración.

A su vez, los procesos de verificación, evaluación y valoración deben estar documentados en su planificación, ejecución y resultados. Además, debe realizarse un seguimiento de los resultados y recomendaciones resultantes de dichos procesos.

[22] Por ejemplo, la implementación del signal-protocol

3 VALIDACIÓN DEL SISTEMA CRIPTOGRÁFICO PARA LA PROTECCIÓN DE DATOS

El responsable y el encargado deben efectuar "*un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento*" (Art. 32). Por motivos de brevedad se ha denominado validación[23] a dicho proceso de verificación, evaluación y valoración. Si el responsable ha decidido emplear cifrado para proteger datos personales, el sistema de cifrado implementado debe ser validado en función de la naturaleza, contexto, ámbito, fines y riesgos del tratamiento.

La relevancia que tiene el cifrado como medida de protección de datos personales en un tratamiento puede variar y, en el mismo sentido, tendrán que adaptarse los requisitos de validación del/los criptosistemas. El nivel de análisis y gestión del proceso de cifrado tendrá que ser proporcional al riesgo para los derechos y libertades de los interesados y al papel del cifrado como medida para la conformidad con el RGPD del tratamiento. La gestión del riesgo determinará cómo se pueden mitigar o evitar el mismo empleando medidas técnicas y organizativas desde las fases iniciales del diseño del tratamiento de datos personales. Esta gestión y la implementación en el tratamiento ha de cumplir con el principio de responsabilidad proactiva/*accountability*, lo que implicará, entre otros, estar documentada y ser verificable.

Como en todo sistema de seguridad, hay que tener en cuenta que la fortaleza y robustez total del sistema de cifrado será igual a la del elemento más débil.

3.1 EVALUACIÓN DE LOS ELEMENTOS DE CIFRADO

A la hora de validar el sistema de cifrado puede ser necesario incluir, entre otros, el algoritmo seleccionado; la implementación del algoritmo; la gestión de claves; la verificación de los procedimientos; la suite de cifrado; el preproceso de los datos; de los protocolos de comunicación; la interacción de los datos cifrados con los aplicativos y el almacenamiento; y, finalmente, la revisión de los aspectos organizativos de la gestión del sistema y el material de cifrado.

Los componentes de un sistema de cifrado se pueden descomponer para un análisis más en detalle. El criterio de descomposición aquí planteado se ha realizado con el objetivo de identificar elementos que se conoce que han sido fuente de vulnerabilidades.

[23] El acto documentado de probar que cualquier procedimiento, proceso, equipo, material, actividad, o sistema conduce realmente a los resultados esperados. Proceso de confirmar que un elemento (un sistema, un producto de trabajo o una parte del mismo) coincide con las necesidades de sus partes interesadas.

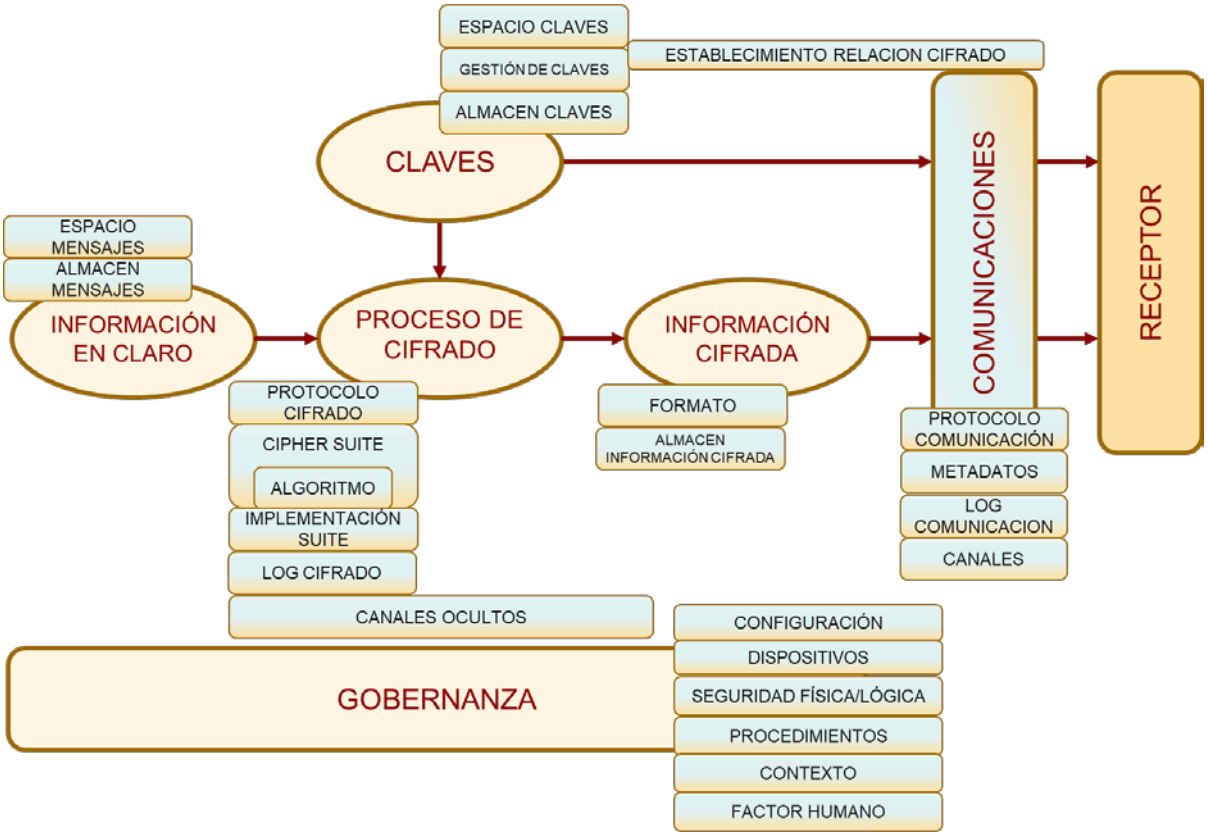


Figura 3 Elementos que forman parte de un sistema de cifrado

3.2 RECOMENDACIÓN EN EL NIVEL DE EVALUACIÓN

Como se ha señalado anteriormente, a la hora de realizar la validación, el nivel de análisis al que se someta el sistema de cifrado dependerá de los siguientes factores:

- Del riesgo que para los derechos y libertades de los interesados podría suponer una brecha en el tratamiento por un problema en el proceso de cifrado,
- De la transcendencia del cifrado como garantía que forma parte de las condiciones para la conformidad con el RGPD del tratamiento,
- Del propósito del sistema de cifrado (almacenamiento, comunicación y/u otros) así como del nivel de cumplimiento que considere adecuado y proporcional.

El nivel de análisis tiene que ser establecido por el responsable y/o encargado del tratamiento, asesorado por el DPD[24] y con el apoyo del responsable de seguridad, mediante un análisis de riesgo para los derechos y libertades que supone el tratamiento en el que se incluye el/los sistemas de cifrado.

Como recomendación, en esta guía se sugieren cuatro niveles distintos de criticidad del sistema de cifrado con relación a un tratamiento de datos personales:

- Como nivel menos crítico, cuando el tratamiento sea de riesgo muy bajo y se incluya el sistema de cifrado como una medida de protección de datos por defecto[25].

[24] En su caso el especialista en protección de datos

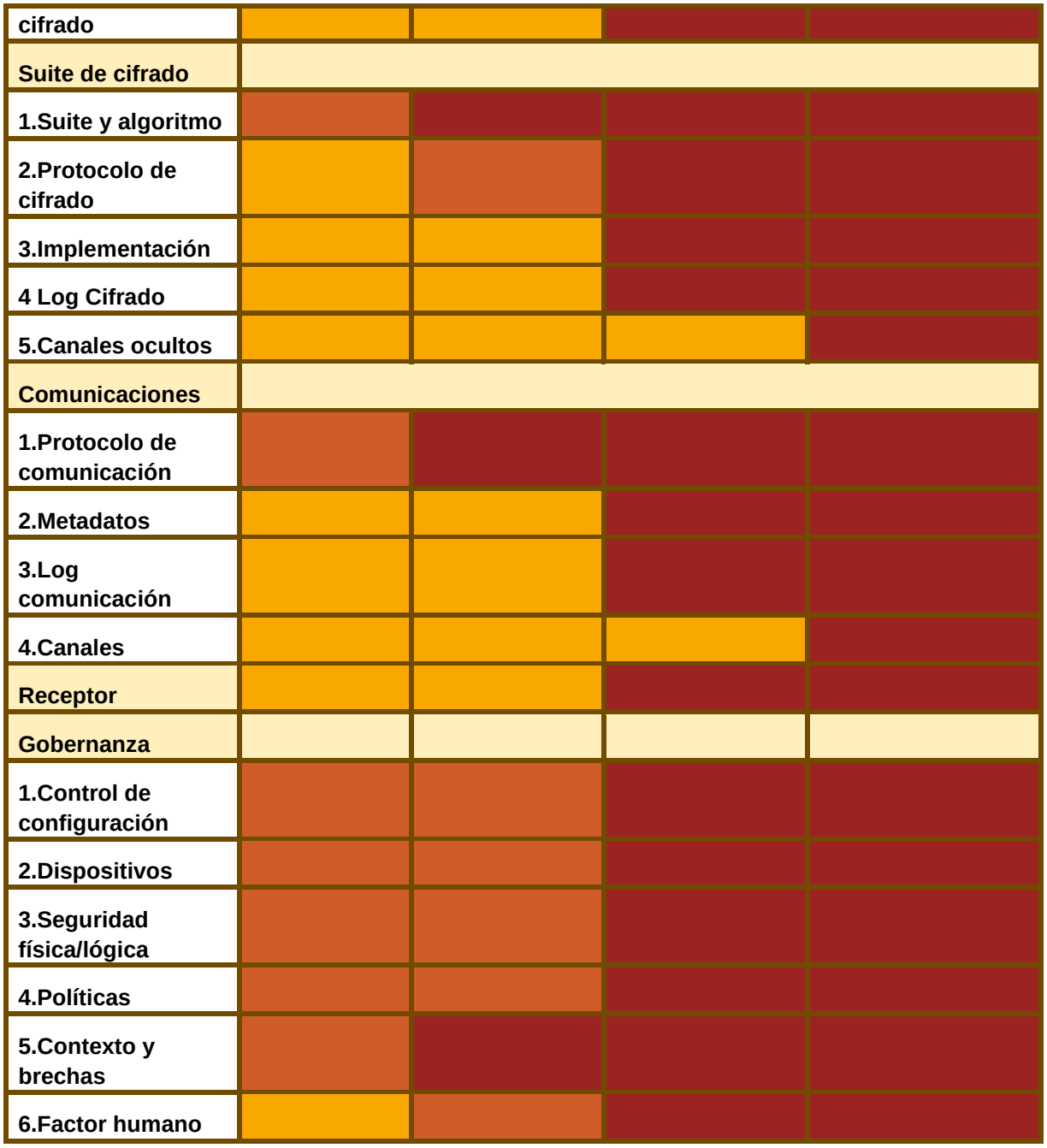
[25] Medidas y garantías establecidas en el tratamiento independientemente del nivel de riesgo del tratamiento y que engloban también las medidas de seguridad por defecto.

- Como de criticidad baja y media, cuando el sistema de cifrados sea una medida que gestiona riesgos medios y bajos en el tratamiento.
- Como de criticidad alta, cuando el sistema de cifrado sea una medida que, de forma complementaria, gestiona el alto riesgo.
- Como altamente crítico, cuando el cifrados sea la garantía principal para gestionar un alto riesgo o que incluso sea la medida principal sobre la que se basa la conformidad con el RGPD del tratamiento.

En función de ello, se sugieren niveles de comprobación de los distintos elementos del sistema de cifrado:

- Opcional: marcado en amarillo.
- Medio: marcado en naranja.
- Alto: marcado en rojo.

	CRITICIDAD DEL CIFRADO COMO MEDIDA QUE GARANTIZA LA PROTECCIÓN DE LOS DERECHOS DEL INTERESADO			
ELEMENTO A EVALUAR	Protección de datos por defecto.	En tratamientos con riesgos medios y bajos.	En tratamientos en los que de forma complementaria gestiona el alto riesgo.	En tratamientos en los que es la medida principal para gestionar un alto riesgo o legitimar el tratamiento.
Claves				
1.Espacio de claves				
2.Gestión de claves				
3.Almacén de claves				
4.Gestión de la relación de cifrado				
Espacio de mensajes				
1.Espacio de Mensajes				
2.Almacenamiento de mensajes				
Información cifrada				
1.Formato				
2.Almacén de				

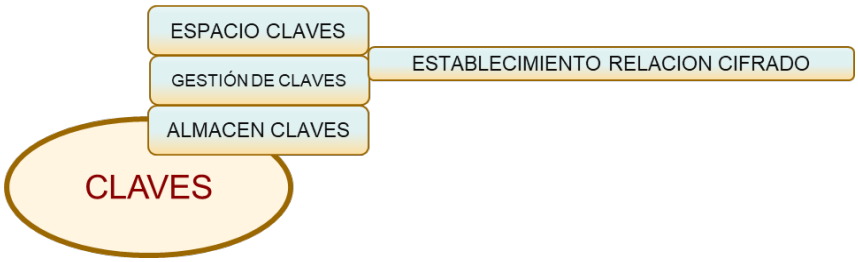


Para cada uno de los elementos, se ha elaborado en este documento una lista de posibles controles. Esta lista no es exhaustiva ni exigible en todos los casos. La lista ha sido realizada para facilitar a los destinatarios de la guía la selección de que comprobaciones pudieran ser las más oportunas para la evaluación de cada elemento concreto en el marco de un tratamiento específico. Los involucrados podrán utilizar esta lista como punto de partida para determinar cuáles de ellos son adecuadas para el tratamiento, cuáles son descartables y, lo más importante, cuáles deben añadir que no se encuentran en la lista de controles sugerida.

Todos los elementos están interrelacionados, de forma que hay comprobaciones que bien pudieran abarcar distintos elementos. Esto se hace evidente en los casos de ejemplo desplegados para cada conjunto de controles, que muestran que es necesaria una visión holística de todo el sistema.

3.3 CLAVES

La fortaleza de un criptosistema descansa en gran medida en la fortaleza de sus claves, y esta depende del espacio de claves, su selección adecuada, su confidencialidad[26] y de un adecuado proceso de gestión de su ciclo de vida[27], en particular, a su debido almacenamiento.



3.3.1 Espacio de claves

El espacio de claves es el conjunto de posibles claves que de forma efectiva (no teórica) se seleccionan en la ejecución real de un sistema de cifrado.

Control	Validación
1. Los requisitos de seguridad de claves han de estar definidos como, p.ej., longitud superior a un número de bits (ver Anexo), formato, etc.	Elija un elemento.
2. Existe un procedimiento para evitar la repetición de claves.	Elija un elemento.
3. No es posible emplear claves generadas a mano.	Elija un elemento.
4. No se emplean contraseñas como claves.	Elija un elemento.
5. No se generan claves a partir de las contraseñas del usuario utilizando funciones de derivación de claves.	Elija un elemento.
6. Hay un procedimiento de detección y eliminación de las claves débiles y previsibles.	Elija un elemento.
7. Está garantizada una alta entropía en el proceso de selección de claves y el recubrimiento potencial de todo el espacio de claves, con una distribución uniforme.	Elija un elemento.
8. Está garantizada la ausencia de correlación entre las claves de distintos usuarios.	Elija un elemento.
9. La generación de claves se produce en un entorno protegido (p.ej. en módulos de seguridad hardware o HSM[28]).	Elija un elemento.
10. La generación de claves estará aislada del entorno de explotación.	Elija un elemento.
11. La generación de claves protege el secreto hacia adelante[29].	Elija un elemento.
12. La generación de claves protege el secreto futuro[30].	Elija un elemento.
13. Los mecanismos de generación de claves estarán certificados y sometidos a la normativa sectorial que sea de aplicación.	Elija un elemento.
14. Si las claves generadas deben o no deben sustanciarse en soportes	

[26] En caso de criptosistemas asimétricos únicamente con relación a la clave privada.
[27] Aunque en algunos casos tienen elementos en común, no hay que confundir las claves con las contraseñas.
[28] https://es.wikipedia.org/wiki/HSM
[29] Si una clave cualquiera, o conjunto de claves, es comprometida, no es posible comprometer las claves pasadas. Es decir, el conocimiento de una clave no permite descubrir claves antiguas con las que se ha cifrado texto con anterioridad.
[30] Si una clave cualquiera, o conjunto de claves, es comprometida, no es posible que un tercero deduzca las claves futuras que se van a generar en la relación de claves

físicos o tokens.	

Entorno ofimático:

Las claves generadas a mano o derivadas de las contraseñas empleadas son vulnerables a ataques de ingeniería social y han sido objeto de análisis sicológico. Incluso se ha desarrollado un término "password psychology" para estudiar los mecanismos internos para elaborarlas. La información publicada en redes sociales, o el análisis de las contraseñas utilizadas por el mismo usuario en cualquier otro servicio, pueden dar mucha información para dirigir ataques de fuerza bruta.

Generadores de claves:

Son dispositivos de almacenamiento local fabricados por diversas firmas tecnológicas, que proporcionan lo que sus creadores llaman "protección de datos de grado militar"; utilizan el algoritmo PBKDF2 como función de derivación de claves realizando 1000 iteraciones de MD5 para derivar la clave de cifrado. La "sal" utilizada para derivar las claves es constante y está codificado en todas las soluciones y todos los proveedores, lo que hace que sea más fácil para un actor determinar la contraseña de usuario[31].

Generación de claves a partir de biometría:

La generación de claves utilizando patrones biométricos (Genkey Biohash Key Creation) podría presentar riesgos relacionados con la corrección de los algoritmos, la tasa de falsos positivos, además de riesgo de privacidad pues pueden revelarse características biométricas de los sujetos. Son susceptibles de ataques de inversión y otros[32].

Criptomonedas:

En wallets digitales de criptomonedas se han deducido claves por la utilización de procedimientos demasiado simples en su generación, como las brain wallets, u otros métodos de simplificación que generan claves débiles (truncamientos, etc.)[33].

Comunicaciones WiFi:

En algunos routers empleados para dar acceso WiFi dentro de las entidades utilizan unos mecanismos de generación de claves con una entropía muy baja que permiten ataques sencillos al protocolo WPS[34].

3.3.2 Gestión de claves

El sistema de cifrado ha de tener un proceso de gestión de claves, y este apartado se refiere a dicho proceso de gestión. Por su especificidad, se desarrolla a continuación:

[31] https://noticiasseguridad.com/vulnerabilidades/el-cifrado-en-dispositivos-de-almacenamiento-western-digital-y-sandisk-tiene-vulnerabilidades-criticas/
[32] https://www.usenix.org/legacy/event/sec08/tech/full_papers/ballard/ballard_html/index.html
[33] https://www.securityweek.com/most-bitcoin-brain-wallets-drained-attackers
https://www.wired.com/story/blockchain-bandit-ethereum-weak-private-keys/
https://www.ise.io/casestudies/ethercombing/
https://cointelegraph.com/news/blockchain-bandit-how-a-hacker-has-been-stealing-millions-worth-of-eth-by-guessing-weak-private-keys
[34] https://www.dragonjar.org/rompiendo-redes-inalambricas-wpa-y-wpa2-con-wps-en-segundos.xhtml

Control	Validación
15. Está documentada la gestión y el ciclo de vida de la relación de claves y certificados: generación, distribución almacenamiento, cambio o actualización, revocación, gestión de claves comprometidas, olvidadas o perdidas, periodos de activación, caducidad, recuperación de claves perdidas o corrompidas, depósito[35], backup y destrucción de claves.	Elija un elemento.
16. Existen extractos de la documentación de la gestión orientados a los distintos roles intervinientes en el proceso de cifrado.	Elija un elemento.
17. Si no se emplea un soporte criptográfico o token, la introducción de la clave y su representación en pantalla no ha de realizarse en un formato legible para el resto de las personas o usuarios que puedan encontrarse alrededor.	Elija un elemento.
18. La distribución interna de claves se realiza mediante canales confidenciales y autenticando a los receptores.	Elija un elemento.
19. Existen procedimientos para formar a los usuarios de que no hay que desvelar nunca las claves o contraseñas a terceros que lo soliciten, incluso si se identifican como administradores del servicio.	Elija un elemento.
20. Existe un procedimiento de gestión de usuarios, tanto para la autorización como para los procedimientos de baja o que han cesado en sus privilegios de forma temporal (ausentes) o permanente.	Elija un elemento.
21. Existe un procedimiento que define el uso de claves que limita la reutilización en múltiples mensajes, el uso en procedimientos y sistemas distintos o en cometidos distintos[36].	Elija un elemento.
22. Existe un procedimiento que garantiza una gran distancia[37] entre dos claves de uso consecutivo[38].	Elija un elemento.
23. Existe una estructura piramidal/jerárquica de claves.	Elija un elemento.
24. Existe un protocolo de revocación de claves o certificados que contemple, no solo el tiempo de uso, sino la cantidad de información intercambiada, el contexto de brechas o ataques, la sensibilidad de la información, etc.	Elija un elemento.
25. Las claves o certificados revocadas que deben ser almacenadas, lo serán en medios aislados de los de explotación.	Elija un elemento.

Reutilización de claves:

Una clave queda expuesta cuando se usa, y resulta más comprometida cada vez que se reutiliza. Por ello, una aproximación para sistemas que requieren una mayor fortaleza es el uso de los sistemas OTP (One Time Password), que limita el tiempo de vida de la clave para cifrar un único mensaje.

Entorno ofimático:

No se deben intercambiar contraseñas en texto claro utilizando servicios de mensajería electrónica. En cualquier caso, nunca se deben enviar las claves en las mismas comunicaciones que los elementos cifrados, sino que se deben enviar de forma independiente por otros canales seguros.

[35] https://www.dit.upm.es/~pepe/401/index.html#!3677
[36] Autenticación, transmisión, almacenamiento, distribución de claves, etc.
[37] Distancia de Hamming
[38] En el caso de claves de texto, dos claves consecutivas han de tener, como mínimo, un 50% de caracteres diferentes a los de la clave anterior.

Redes WiFi:

En el cifrado WEP (redes WiFi) la reutilización de claves y vectores de inicialización posibilita ataques de fuerza bruta sencillos para la obtención de la clave[39].

3.3.3 Almacén de claves

Las claves simétricas, o los pares de claves públicas y privadas, han de registrarse con garantías, tanto de confidencialidad como de recuperación. El almacenamiento de las claves no sólo es un problema del individuo que cifra sus propios datos, sino también de la organización en la medida que ha de ser capaz de recuperar datos cifrados por sus empleados, disponiendo de un almacén de claves.

La gestión del almacenamiento de claves sería un caso particular del apartado anterior, pero se desarrolla de forma independiente por razones de claridad.

Control	Validación
1. Las claves no se registran en claro en ningún tipo de soporte.	Elija un elemento.
2. Las claves no se almacenan de forma no volátil o externa cuando la clave no está cifrada (clave envuelta[40]).	Elija un elemento.
3. Existe una gestión específica de claves que se emplean para proteger claves.	Elija un elemento.
4. Hay una protección o dispositivos criptográficos (HSM, hardware security module) para preservar la confidencialidad de las claves.	Elija un elemento.
5. Los propios mecanismos de protección están sometidos a revisión periódica.	Elija un elemento.
6. Existe procedimientos de depósito, backup y de recuperación de claves.	Elija un elemento.
7. El acceso a las claves está sujeto a control y registro de accesos.	Elija un elemento.
8. Existen procedimientos automáticos para detectar y alertar de accesos indebidos a los almacenes de clave.	Elija un elemento.
9. Existen procedimientos de eliminación y borrado seguro de claves.	Elija un elemento.

Entorno ofimático:

Resulta típico utilizar notas en texto claro tanto en formato papel como electrónico en un lugar sin controles de acceso, por ejemplo, en un post-it, en una nota almacenada en una carpeta de Dropbox compartida, en el correo electrónico, etc. En muchos casos no es error del usuario, sino de la carencia de protocolos, políticas y herramientas para el almacenamiento y la gestión de claves en la organización.

[39] https://wiki.elhacker.net/seguridad-wireless/introduccion/vulnerabilidades-del-cifrado-wep

[40] Clave de cifrado de clave (KEK, Key Encryption Key) o clave de envoltura de clave son claves que se utilizan para proteger la confidencialidad de claves. También se utilizan en los procesos de intercambio de claves como claves de transporte.

Criptomonedas:

Un ciudadano extravió las claves que le permitían acceder a sus bitcoins, al desechar en la basura el disco en las que las tenía almacenadas. El valor de los bitcoins, así inaccesibles, llegó a alcanzar los 280 millones de euros[41].

Validación de los HSM:

Utilizar un dispositivo HSM no es una garantía absoluta. Dichos dispositivos también se encuentran sometidos a fallos, vulnerabilidades y ataques y, por tanto, también hay que implementar medidas para validar y acreditar su fortaleza ante distintos vectores de ataque, incluidos los que se derivan de errores de implementación, como aquellos que han permitido reinstalar su software[42].

3.3.4 Gestión de la relación de cifrado y certificados

Cuando el cifrado implica la relación de más de un interviniente, es necesario el establecimiento de una relación de cifrado entre dos (o más) interlocutores. El establecimiento de la relación de cifrado implica más que intercambiar claves, también implica consensuar los algoritmos de cifrado, así como otros aspectos de la suite de cifrado y del protocolo de utilización del sistema:

Control	Validación
1. Si dos partes acuerdan intercambio de información para establecer una relación de claves, ambos han de estar seguros de la identidad y origen de los mensajes de la otra parte.	Elija un elemento.
2. En el caso de autenticación en una infraestructura de clave pública (PKI), esta ha de ser fiable.	Elija un elemento.
3. En el caso de claves simétricas, si dos partes acuerdan el intercambio de información para establecer una relación de claves, las claves que establezcan entre ambos han de ser distintas a las que establezca una de las partes con otra tercera parte.	Elija un elemento.
4. Si hay claves comunes ha de haber claves distintas para diferentes grupos no autorizados a comunicarse entre sí	Elija un elemento.
5. Los certificados recibidos y la cadena de confianza se validan apropiadamente.	Elija un elemento.
6. Mientras dos partes están realizando el intercambio de información para establecer una relación de claves, ninguna otra tercera entidad ha de ser capaz de inferir la identidad de ambas partes.	Elija un elemento.
7. El establecimiento de la relación de claves (algoritmos, elementos de la suite, etc.) se ha de realizar de forma confidencial.	Elija un elemento.

[41] https://www.cnbc.com/2021/01/15/uk-man-makes-last-ditch-effort-to-recover-lost-bitcoin-hard-drive.html
[42] https://www.blackhat.com/us-19/briefings/schedule/?hootPostID=db681a52c6a321681e1f9281b5124457#everybody-be-cool-this-is-a-robbery-16233

Entornos ofimáticos:

Ataques NTLM\f “Acronimos” Relay en controladores de dominio de Windows son posibles si no se activan protecciones relacionadas con firmas con certificados[43].

Caducidad de certificados:

Un proveedor de sistemas de comunicaciones interrumpió el servicio a 32 millones de usuarios de distintas compañías de comunicaciones debido a una mala gestión de la caducidad de los certificados digitales[44].

Compromiso de certificados:

La posibilidad de compromiso de certificados (por robo, ingeniería social[45], corrupción[46], fugas de información[47]…) es un hecho que va más allá de conseguir acceso a los sistemas, y se ha utilizado para firmar aplicaciones maliciosas[48], para firmar malware[49] que puede conducir a perdida de la confidencialidad o la disponibilidad de datos personales (ransomware)

3.4 MENSAJES EN CLARO

El mensaje en claro es aquel mensaje que quiero cifrar con el objeto de mantenerlo de forma confidencial en almacenamiento o en su transmisión.

3.4.1 Espacio de mensajes

El espacio de mensajes es el conjunto de mensajes posibles que se esté cifrando. Cuanto más predecibles sean los mensajes, menor será la fortaleza de dicho mensaje. Dicha predictibilidad tiene más impacto cuanto más afecte a la parte inicial del mensaje a transmitir. Por ejemplo, los formatos estándar para almacenar texto, video, imágenes o correos suelen tener cabeceras que son siempre las mismas (o con pequeñas variaciones dependiendo del usuario) que hacen más fácil un criptoanálisis.

Además, determinadas herramientas realizan un preproceso de los mensajes antes de ser cifrados que puede incrementar, pero también en algunos casos disminuir, la fortaleza del mismo.

[43] https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429
[44] https://www.venafi.com/blog/cellular-outage-32-million-brits-caused-expired-certificate
[45] https://www.incibe.es/protege-tu-empresa/avisos-seguridad/multiples-campanas-phishing-intentan-obtener-las-credenciales-tu
[46] https://www.xataka.com/seguridad/buscamos-empleados-microsoft-apple-asi-como-lapsus-esta-hackeando-a-big-tech-dentro
[47] https://9to5google.com/2022/12/01/android-security-leak-samsung-lg/
[48] https://www.linkedin.com/pulse/stolen-security-certificate-compromises-privacy-palanisamy
[49] https://www.malwarebytes.com/blog/news/2022/03/stolen-nvidia-certificates-used-to-sign-malware-heres-what-to-do

Control	Validación
1. No existen o se evitan cabeceras estáticas en los mensajes o conjunto de mensajes a cifrar.	Elija un elemento.
2. En los mensajes se evita una estructura previsible e identificable en los mensajes, tales como patrones, abreviaturas, información pública o evidente.	Elija un elemento.
3. Si el mensaje en claro está formado por un conjunto de ficheros se preprocesan los mismos para ocultar.	Elija un elemento.
4. Se realiza una compresión del mensaje en claro antes de cifrarlo.	Elija un elemento.
5. El ajuste del mensaje al tamaño de bloque del algoritmo de cifrado se realiza utilizando rellenos adecuados (padding) y sin vulnerabilidades conocidas.	Elija un elemento.
6. El espacio de mensajes garantiza por diseño una alta entropía (p.ej. con la inclusión de segmentos aleatorios sobre todo al comienzo y al final).	Elija un elemento.

Entornos ofimáticos:

Al cifrar dos documentos distintos, pero generados por el mismo procesador de textos, el mismo autor y la misma clave, los primeros bloques de los documentos cifrados son exactamente iguales. Esto es debido a que las herramientas de generación de documentos, como procesadores de textos, hojas de cálculo, etc., suelen tener un conjunto de cabeceras estáticas. Dichos documentos son vulnerables a ataques basados en texto en claro conocido ya que, aunque se cambie de clave, ya se sabe qué contienen los primeros bloques. Si a esto se añade que determinados documentos tienen una estructura estándar en la que los datos que difieren entre dos documentos es mínimo, la vulnerabilidad aumenta. Existen ejemplos de herramientas de descifrado empleando este principio[50].

Protección de campos de un conjunto de datos:

En conjuntos de datos organizados en campos, como nº de teléfono, DNI u otros identificadores, es posible que los campos se cifren de forma individual. En esos casos, hay que tener en cuenta que dichos campos pueden tener muy poca variabilidad. Por ejemplo, el número de combinaciones posibles de un número de teléfono válido es muy bajo desde el punto de vista de un análisis automático (baja entropía).

Límites en la seguridad del cifrado:

La distancia de unicidad, también llamada punto de unicidad, es el valor mínimo de caracteres del texto cifrado que se necesitan para reducir a una el número de claves posibles. A partir de esa cantidad el cifrador es teóricamente rompible teniendo los suficientes recursos. No depende del algoritmo, sino de la entropía del espacio de mensajes y de la longitud real de la clave. Por ejemplo, un texto en castellano cifrado con AES 256 sobrepasa la distancia de unicidad con más de 95 caracteres[51].

3.4.2 Almacenamiento de mensajes en claro

En el caso de servicios de mensajería, documentación remitida de forma cifrada, copias de seguridad protegida o conjuntos de datos remitidos a terceros de forma cifrada, en

[50] https://www.acceis.fr/cracking-encrypted-archives-pkzip-zip-zipcrypto-winzip-zip-aes-7-zip-rar/
[51] https://es.wikipedia.org/wiki/Distancia_de_unicidad#C%C3%A1lculo_en_otros_cifradores

muchos casos la información original podría estar almacenada en forma de un mensaje en claro.

La forma más sencilla para comprometer un mensaje cifrado es directamente acceder al mensaje en claro que lo ha originado. También conocer mensajes en claro sobre otra información que no es el objeto de interés del atacante, puede ser una fuente de información sobre los procesos de gestión de claves y cifrado en general.

Control	Validación
1. Está protegida la confidencialidad del almacenamiento de mensajes permanentes y copias temporales	Elija un elemento.
2. Existe un procedimiento de control de acceso al almacenamiento de mensajes en claro.	Elija un elemento.
3. Existe un registro de acceso al almacenamiento de mensajes en claro.	Elija un elemento.
4. Existen procedimientos automáticos para detectar y alertar de accesos indebidos al almacén de mensajes.	Elija un elemento.
5. Para determinado tipo de mensajes, existen procedimientos de caducidad de mensajes en claro que se transmitieron cifrados.	Elija un elemento.
6. Las copias temporales no son accesibles por terceros o terceras aplicaciones y son sometidas a borrado seguro.	Elija un elemento.
7. El acceso al almacenamiento de mensajes en claro, cuando se habilita, está limitado en el conjunto de aplicaciones que lo pueden explotar.	Elija un elemento.
8. Existen procedimientos de borrado seguro de mensajes en claro y copias temporales	Elija un elemento.
9. No hay vinculación entre los mensajes en claro y las claves utilizadas para cifrarlos.	Elija un elemento.
10. No hay vinculación entre los mensajes en claro y su cifrado.	Elija un elemento.

Mensajería instantánea:

Algunas aplicaciones de mensajería instantánea almacenan los mensajes y/o contenido multimedia en claro en los propios dispositivos, de forma que el ataque a la confidencialidad de los mensajes se realiza sobre dichos almacenamientos antes que sobre los mensajes transmitidos[52].

[52] https://www.makeuseof.com/tag/how-whatsapp-messages-can-hacked/

Discos cifrados:

El cifrado del almacenamiento de un sistema o un soporte de datos removible es una medida básica de seguridad contra robo o extravío. Sin embargo, hay que ser consciente de que solo proporciona cierto grado de seguridad. Una vez abierto el acceso al dispositivo, por ejemplo, iniciando una sesión en el sistema, los datos están disponibles para multitud de aplicaciones, por lo que no pueden considerarse que los datos están cifrados durante la operación normal del sistema[53].

3.5 INFORMACIÓN CIFRADA

Los mensajes cifrados pueden estar almacenados por largo tiempo, en particular cuando se tiene por objetivo el cifrado de la información en reposo, o bien pueden almacenarse por muy cortos intervalos, mientras se encuentra en la cola de transmisión.

3.5.1 Formato

Los mensajes cifrados suelen tener un formato que depende del software de cifrado. En el formato puede incluirse información no cifrada, que facilite la operación diaria con dichos ficheros, pero también que incorpore debilidades en el sistema de cifrado.

Control	Validación
1. El formato del criptograma no incluye información no cifrada, ni relacionada con el proceso o la naturaleza de la información cifrada.	Elija un elemento.
2. No se incluye la clave en la cabecera del texto antes de ser cifrado.	Elija un elemento.
3. Cuando el mensaje cifrado está formado por varios ficheros independientes, no se almacena en claro una descripción de su contenido.	Elija un elemento.
4. En caso de que se empleen técnicas esteganográficas o de cifrado negable, ha sido analizada su efectividad.	Elija un elemento.

Servicios web:

Algunas herramientas de cifrado revelan información en su formato, tales como los JWE, JSON Web Encryption, usados generalmente como tokens de acceso (versión de los JWT, JSON web Tokens con contenido cifrado).

[53] https://www.makeuseof.com/tag/how-whatsapp-messages-can-hacked/ en su apartado 4.

Entorno ofimático:

En algunas herramientas que generan ficheros tipo “zip” cifrados, en la configuración por defecto se revela información en claro sobre el tipo de algoritmo utilizado, versión de la herramienta o incluso los ficheros almacenados y permite utilizar estrategias basadas en una debilidad en el Espacio de Mensajes visto anteriormente.

Mensajería instantánea:

En servicios de mensajería móvil, los primeros caracteres de los mensajes se almacenan también en Notificaciones, cuando la aplicación no está abierta en el celular, de forma que permite recuperar mensajes al margen de cualquier protección, que incluso se creían borrados[54].

3.5.2 Almacén de cifrado

Control	Validación
1. Existen controles de acceso físico y lógico a los repositorios de información cifrada.	Elija un elemento.
2. Existen mecanismos de autenticación que evitan una suplantación del usuario que ha introducido las claves de acceso al almacén de cifrado.	Elija un elemento.
3. No existe otro almacenamiento paralelo en el que es posible encontrar en claro los mensajes cifrados, en todo o en parte.	Elija un elemento.
4. Existe un backup del almacén de cifrado.	Elija un elemento.

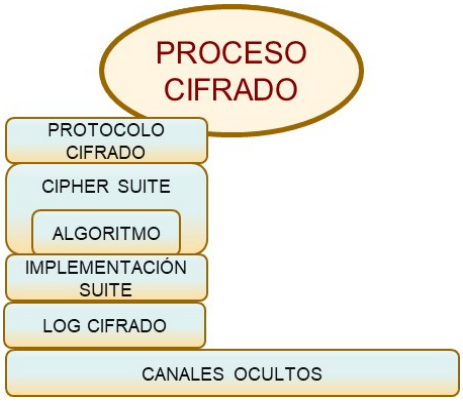
Acceso no autorizado:

La suite de cifrado de discos Truecrypt fue descatalogada al descubrirse que era posible, una vez que un usuario introducía la clave para acceder al contenido cifrado, realizar accesos no autorizados por terceros a los contenidos[55].

3.6 SUITE DE CIFRADO

La suite de cifrado está formada por todos los componentes software/hardware/procedimientos que hay alrededor del algoritmo teórico de cifrado y que van a determinar su operación. El algoritmo, p.ej. AES, se va a implementar utilizando una serie de librerías y complementos necesarios para la ejecución real del mismo. Una propuesta de clasificación de dichos complementos es la siguiente:

[54] https://www.xataka.com/basics/recuperar-mensajes-borrados-whatsapp
[55] https://thehackernews.com/2015/09/truecrypt-encryption-software.html



3.6.1 Suite y algoritmo

Los algoritmos se ejecutan sobre implementaciones concretas. Además, es necesario utilizar múltiples elementos que permiten la implementación del sistema de cifrado sobre un sistema concreto: generadores de números aleatorios, números primos, relleno de bloques, extensión de claves, etc. Todos ellos pueden ser fuente de vulnerabilidades.

Control	Validación
1. Los elementos de la suite están identificados en su nombre y versión e inventariados. En particular, algoritmos de cifrado, MAC, intercambio de claves, padding, generadores de números aleatorios, generadores de claves, certificados, protocolos automáticos, herramientas de gestión de claves, etc.	Elija un elemento.
2. La seguridad de la suite es demostrable.	Elija un elemento.
3. Están identificados los criterios para determinar los elementos de la suite adecuados para el contexto de la aplicación y la vida de los datos personales.	Elija un elemento.
4. Los elementos de la suite están adecuadamente certificados y cumplen con la normativa sectorial.	Elija un elemento.
5. Están actualizados los estados de las certificaciones.	Elija un elemento.
6. No se emplean en la suite algoritmos comprometidos, no certificados o desarrollados “ad-hoc”.	Elija un elemento.
7. La generación de números aleatorios ha de ser adecuada, con un algoritmo fuerte (software o hardware), certificado o de acuerdo con la normativa (ENS), y que supere los test de siguiente bit y el compromiso del estado.	Elija un elemento.
8. Las semillas de la generación de números aleatorios deben ser configurables por el usuario o, existe una funcionalidad de creación de la semilla con la suficiente entropía e impredecibilidad.	Elija un elemento.
9. La generación de números primos ha de ser no predecible.	Elija un elemento.
10. Está controlada la configuración de la suite utilizada para cifrar cada mensaje en claro.	Elija un elemento.
11. Existe backup de los elementos de la suite.	Elija un elemento.
12. La información sobre la suite es confidencial.	Elija un elemento.

Acceso a la nube:

El acceso a servicios remotos o en la nube se realiza por herramientas que permiten configurar la suite de cifrado que se emplea. La configuración por defecto se debe ajustar para que solo se empleen aquellos elementos de la suite que cumplan con los requisitos de seguridad[56].

3.6.2 Protocolo de cifrado

El protocolo de cifrado está formado por procesos automatizados (que formarán parte de la suite en sentido amplio) y no automatizados que se empleen para ejecutar las operaciones de cifrar y descifrar información.

Control	Validación
1. El protocolo ha de estar bien documentado, auditado por terceros o certificado.	Elija un elemento.
2. El protocolo no utiliza tratamientos de bloque inseguros. (p.ej. ECB)	Elija un elemento.
3. El protocolo incluye mecanismos de cifrado autenticado. (p.ej. GCM)	Elija un elemento.
4. El protocolo garantiza que no se cifra sólo un fragmento del mensaje.	Elija un elemento.
5. El protocolo garantiza que no se envía el mismo mensaje cifrado y sin cifrar.	Elija un elemento.
6. El protocolo garantiza que no se cifra el mismo mensaje con distintas claves o algoritmos.	Elija un elemento.
7. El protocolo garantiza que no se use la misma clave para distintos destinatarios.	Elija un elemento.
8. El protocolo garantiza un máximo de información cifrada con la misma clave.	Elija un elemento.
9. El protocolo garantiza que no se puede reemplazar, eliminar o desordenar distintos bloques del texto cifrado sin ser detectado.	Elija un elemento.

Conjuntos masivos de datos:

Uno de los límites para un cifrado seguro es no sobrepasar la cantidad de información cifrada con la misma clave a una potencia de 2 de la mitad del tamaño de bloque de cifrado. Este límite, que se conoce como el "límite del cumpleaños" puede ser alcanzado fácilmente con cifradores de pequeño tamaño de bloque, como los basados en DES y obliga al cambio de clave[57].

[56] https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/restrict-cryptographic-algorithms-protocols-schannel
[57] https://sweet32.info/

Pérdida de integridad en comunicaciones:

La utilización de modos de cifrado ECB o no autenticados como GCM permite realizar ataques a la integridad de los conjuntos de mensajes transmitidos, permitiendo intercalar información falsa que puede alterar el significado de la información y tener efectos en cascada sobre el tratamiento de datos personales[58].

3.6.3 Implementación

La implementación es la traducción al mundo real de los diseños, algoritmos y herramientas diseñadas de forma teórica. Esto implica una codificación concreta, la definición de los parámetros del algoritmo y el empleo en sobre un sistema concreto. Puede haber una gran distancia entre la protección teórica y la protección efectiva debido a limitaciones introducidas en la implementación de los algoritmos y los problemas en la integración con el resto del sistema.

Control	Validación
1. Se han realizado pruebas de vulnerabilidad de los elementos Hw/Sw que componen el sistema de cifrado.	Elija un elemento.
2. Se ha comprobado que no existe persistencia en la memoria de claves o textos claros utilizados en el proceso de cifrado.	Elija un elemento.
3. Está analizado que no hay claves incluidas en el código. (hardcoded)	Elija un elemento.
4. Existe un procedimiento de comprobación para evitar el filtrado de la información del comportamiento del sistema.	Elija un elemento.
5. Existen medidas para impedir la detección y manipulación de la implementación: operaciones de duración no determinista, blindaje de circuitos, homogeneización de consumos, modificar implementación de algoritmos registrados, añadir ruido y operaciones inútiles.	Elija un elemento.
6. En las implementaciones se utilizan librerías adecuadas, certificadas (FIPS 140-2, 197), o autorizadas (CCN-STIC-807).	Elija un elemento.
7. La generación de vectores de inicialización, “salt” y “nonces” garantiza que sean seguros (tamaños mínimos y no repetidos) y no se reutilizan.	Elija un elemento.
8. Los métodos de padding de los bloques están actualizados y adecuados para el tipo de tratamiento. Por ejemplo, no usar PKCS v1 o v1.5.	Elija un elemento.
9. Las funciones hash utilizadas son adecuadas para el uso criptográfico, son modernas y no obsoletas. Por ejemplo, no usar MD5 o SHA1.	Elija un elemento.
10. La implementación de la validación de certificados es segura.	Elija un elemento.

Aplicaciones corporativas:

Una aplicación corporativa de uso extendido mantuvo una clave de cifrado escrita en el propio código para proteger los datos almacenados (en reposo). Una inspección del código permitía acceder a la información de configuración confidencial almacenada[59].

[58] https://sysfatal.github.io/maleable.html
[59] https://www.cvedetails.com/cve/CVE-2016-3684/

Entorno ofimático:

El controlador de un sistema operativo utilizado por proyectos derivados de Truecrypt 7 era vulnerable a un ataque de elevación local de privilegios al abusar de las funciones de creación de enlaces simbólicos de letras de unidad para reasignar la unidad principal del sistema[60].

Falta de revisión de la implementación:

En el caso de una plataforma de videojuego online que, aunque empleaba claves asimétricas generadas con curvas elípticas, se determinó la vulnerabilidad de las mismas debido a que la semilla de generación de claves era constante en todas las implementaciones de la misma, introduciendo determinismo en el espacio de claves[61].

Comunicaciones:

Una empresa de sistemas proporcionaba una RTU (Unidad de Terminal Remota) con cifrado SSH en el que la clave privada de acceso estaba escrita en el propio código y no se actualizaba si se empleaba la configuración por defecto[62].

Mensajería instantánea:

En 2019 se descubrió que el envío de MP4 maliciosos podría generar en un servicio de mensajería instantánea un desbordamiento de buffer y así permitir el acceso a los mensajes[63].

3.6.4 Log de cifrado

La operación del sistema de cifrado genera ficheros de bitácora o de "log" que serán esenciales en la validación y auditoría del sistema, sin embargo, pueden convertirse a su vez en fuente de vulnerabilidades.

Control	Validación
1. Existe un log de las actividades de cifrado.	Elija un elemento.
2. No han de almacenar claves, texto en claro o cifrado o cualquier otra información que pueda servir para el criptoanálisis.	Elija un elemento.
3. Han de minimizarse los datos registrados, con criterios estrictos de destrucción, almacenaje y copia.	Elija un elemento.
4. Los logs de cifrado han de estar protegidos en cuanto a su confidencialidad e integridad.	Elija un elemento.
5. Está garantizado un control de acceso muy restrictivo y con trazabilidad de este, con alertas en tiempo real.	Elija un elemento.

[60] https://www.exploit-db.com/exploits/38403
[61] https://www.edn.com/the-sony-playstation-3-hack-deciphered-what-consumer-electronics-designers-can-learn-from-the-failure-to-protect-a-billion-dollar-product-ecosystem/
[62] https://www.cisa.gov/uscert/ics/advisories/icsa-22-179-06
[63] https://thenextweb.com/news/whatsapp-fixes-bug-that-would-have-let-hackers-exploit-devices-using-mp4-files

Comunicaciones:

Una implementación de SSH almacenaba la clave privada en el fichero de log, accesible a todos los usuarios que podían ganar acceso al mismo[64].

3.6.5 Canales ocultos

Un canal oculto o encubierto es cualquier canal de comunicación que puede ser explotado por un proceso para transferir información de forma que viole la política de seguridad del sistema. Esto puede ser debido malos diseños del sistema sobre el que se ejecuta el cifrado o por la existencia de puertas traseras.

Control	Validación
1. Existe un análisis de canales ocultos en la suite.	Elija un elemento.
2. Existe un análisis de canales ocultos en los protocolos automatizados y no automatizados.	Elija un elemento.
3. Existe un análisis de canales ocultos en los canales de comunicación, como pueden ser los mensajes de error.	Elija un elemento.
4. Existe un análisis de canales ocultos en la implementación en software (librerías) y hardware.	Elija un elemento.
5. Existe un análisis de canales ocultos en el sistema operativo que ejecuta el sistema de cifrado.	Elija un elemento.
6. En tratamientos implementados sobre sistemas de información complejos, incluso para almacenamiento en reposo, hay que determinar la seguridad de los flujos de información entre los balanceadores de carga, servidores web, sistema de back-end, y otros internos y externos[65].	Elija un elemento.
7. Si la organización emplea canales ocultos en el sistema de cifrado para supervisión e inspección de contenido, la supervisión ha de ser en tiempo real, han de minimizarse los datos registrados, con criterios estrictos de destrucción temprana, los registros han de estar protegidos en cuanto a confidencialidad, y debe estar garantizado un control de acceso muy restrictivo y con trazabilidad de este, con alertas en tiempo real.	Elija un elemento.

Mensajería instantánea:

Una red social proporcionaba un sistema de mensajería cifrado extremo-a-extremo. Sin embargo, los emoticonos no están insertados en el mensaje, sino solo un vínculo a la imagen del mismo. Cuando se descargaba un mensaje, lo primero a realizar era la petición al servidor de los dibujos de los emoticonos contenidos en el mensaje, lo que revelaba mucha información sobre la conversación.

[64] https://www.cve.org/CVERecord?id=CVE-2018-1999036
[65] También está relacionado con la existencia de logs de material cifrado y de mensajes en claro.

Canales ocultos:

Un ataque de oráculo es un tipo de ataque de canal oculto (side-channel) que aprovecha que el protocolo o sistema permite deducir si el adversario está cerca o no de conseguir un objetivo. Por ejemplo, el ataque de Vaudenay[66] consiste en saber si un mensaje cifrado que envía el atacante tiene bien formado el padding o no. Esto lo puede saber si el servidor devuelve un error que permite diferenciar si hay un error de padding o si el error es de otro tipo (por ejemplo, del MAC). También se podría saber midiendo el tiempo que tarda el servidor en responder a una petición, etc.

Comunicaciones:

Aunque las especificaciones de TLS requieren que los servidores comprueben el padding, algunas implementaciones no lo validan correctamente. POODLE[67] "Padding Oracle On Downgraded Legacy Encryption") es una vulnerabilidad de seguridad que se aprovecha del downgrade a SSL 3.0., lo que hace que algunos servidores sean vulnerables a POODLE incluso si desactivan SSL 3.0.

3.7 COMUNICACIONES

El sistema de cifrado puede estar orientado a la protección de datos en reposo, pero uno de los propósitos frecuentes en un sistema de cifrado es la protección de los datos que se intercambian a través de redes de comunicaciones. El propio hecho de la comunicación puede implicar vulnerabilidades específicas que no aparecen en la protección de información en reposo.

3.7.1 Protocolo de comunicaciones

El protocolo de comunicaciones es el sistema de reglas que permiten que dos o más entidades de un sistema de comunicación intercambien mensajes entre ellas. En el caso que nos ocupa incluirá, también, el establecimiento de la relación de cifrado, así como los propios mensajes cifrados.

Control	Validación
1. La autenticación se garantiza en el establecimiento de cada sesión y en cada intercambio dentro de una sesión.	Elija un elemento.
2. Están implementados procedimientos para prevenir y detectar suplantaciones de identidad de los interlocutores. (MITM)	Elija un elemento.
3. Están implementados procedimientos para prevenir y detectar retardos, reordenación o supresión de fragmentos del texto cifrado, modificación selectiva de la información cifrada, fabricación de mensajes ficticios con fragmentos de mensajes auténticos, invención de mensajes, repetición de mensajes, reflexión (devolución del mensaje al remitente), alteración del destinatario del mensaje, etc.	Elija un elemento.

[66] https://sysfatal.github.io/oracle.html
[67] https://es.wikipedia.org/wiki/Ataque_POODLE

SSL/TLS:

Están documentados numerosos problemas de seguridad de los protocolos SSL/TLS. En la nota al pie se describen los ataques más significativos (recientes) centrados en anular la criptografía[68].

3.7.2 Metadatos

Los metadatos en las comunicaciones electrónicas son los datos procesados en una red de comunicaciones con el propósito de transmitir, distribuir o intercambiar un mensaje, en este caso cifrado. Esto incluye los datos utilizados para determinar e identificar el origen y el destino de una comunicación, datos sobre la ubicación del dispositivo, y la fecha, hora, duración y tipo de comunicación[69].

Control	Validación
1. Están minimizados y son conocidos los metadatos en las comunicaciones.	Elija un elemento.
2. El impacto de los metadatos en el criptoanálisis se ha analizado.	Elija un elemento.

Redes WiFi:

En algunas implementaciones de fabricantes de routers WiFi, que emplean cifrado WPA/WPA2, es posible aprovechar los datos de los campos opcionales de las tramas de control emitidas para realizar ataques de tipo PMKID[70].

3.7.3 Log de comunicación

Las comunicaciones también generan ficheros de bitácora o de "log" que serán esenciales en la supervisión y auditoría del sistema, que pueden convertirse a su vez en fuente de vulnerabilidades.

Control	Validación
1. Los ficheros de log no han de almacenar claves ni texto cifrado.	Elija un elemento.
2. Cuando la comunicación no sea directa, hay que conocer y controlar la información de log que se genera en los sistemas de reenvío.	Elija un elemento.
3. Han de minimizarse los datos registrados, con criterios estrictos de destrucción, almacenaje y copia.	Elija un elemento.
4. Han de estar protegidos en cuanto a confidencialidad.	Elija un elemento.
5. Está garantizado un control de acceso muy restrictivo y con trazabilidad de este (alarmas para accesos sospechosos).	Elija un elemento.
6. La herramienta de gestión de logs está auditada y/o certificada.	Elija un elemento.
7. Existen procedimientos para prevenir ataques en la gestión de logs tipo "log poisoning".	Elija un elemento.

[68] Seguridad del protocolo SSL/TLS. Ataques criptoanalíticos modernos. Autor: Dr. Alfonso Muñoz https://raw.githubusercontent.com/mindcrypt/libros/master/Book. Seguridad en el protocolo SSL-TLS. Dr. Alfonso Muñoz - 05082021.pdf

[69] Definición procedente de la Propuesta de Reglamento de ePrivacy

[70] https://kalitut.com/pmkid-attack/

Logs de comunicaciones:

Una gestión inadecuada de los logs puede ser aprovechada para explotar vulnerabilidades de tipo log poisoning, presente en algunas aplicaciones[71].

3.7.4 Canales

El canal es el soporte físico (y sus extensiones virtuales) que permite el intercambio efectivo de información entre dos interlocutores. El canal puede tener formas muy complejas en Internet, con multitud de intervinientes intermedios que, en muchos casos, podrían resultar transparentes para el usuario.

Control	Validación
1. Están implementados procedimientos para prevenir y detectar el uso de canales abiertos.	Elija un elemento.
2. Están implementados procedimientos para prevenir y detectar canales privados.	Elija un elemento.
3. Están implementados procedimientos para prevenir y detectar la escucha y recogida de información cifrada.	Elija un elemento.
4. Están implementados procedimientos para prevenir y detectar el análisis de tráfico y la vinculación de información.	Elija un elemento.
5. Están implementados procedimientos para prevenir y detectar ataques a los servicios DNS.	Elija un elemento.
6. Están implementados procedimientos para prevenir y detectar ataques de denegación de servicio.	Elija un elemento.
7. Están implementados procedimientos para prevenir y detectar cortes de los canales (físicos y lógicos).	Elija un elemento.
8. Están implementados mecanismos de segmentación de red física y/o virtual (VLAN\f “Acronimos”).	Elija un elemento.

Escuchas en la infraestructura de red:

Dispositivos de tapping/sniffing en los cables ethernet o de fibra. Dispositivos de WiFi-jamming (que provocan denegaciones de servicio) o sniffing.

Ataques de de-autenticación WiFi junto con puntos de acceso falsos (WiFi de-auth y evil-twin[72])

3.8 RECEPTOR

El receptor es aquel que va a recibir los mensajes cifrados, en algunos casos tendrá las claves de descifrado y almacenes de mensajes cifrados y en claro, por lo tanto, tendrá que cumplir con las mismas garantías que el emisor.

Control	Validación
1. El receptor está autenticado.	Elija un

[71] https://www.cvedetails.com/cve/CVE-2019-11642/ https://www.cvedetails.com/cve/CVE-2021-40323/ https://nvd.nist.gov/vuln/detail/CVE-2021-40323

[72] https://www.nextgov.com/cybersecurity/2020/09/interior-ig-team-used-evil-twins-and-200-tech-hack-department-wi-fi-networks/168521/

	elemento.
2. Las sesiones abiertas con el receptor caducan. Las claves de sesión usadas no son predecibles.	Elija un elemento.
3. La re-autenticación durante una sesión abierta se realiza aleatoriamente.	Elija un elemento.
4. El nivel de conformidad del receptor en cuanto al sistema de cifrado equivale al del emisor.	Elija un elemento.
5. El receptor ha sido evaluado con auditorías y/o certificaciones.	Elija un elemento.
6. El personal del receptor ha realizado formación y dispone de políticas y manuales prácticos para el adecuado manejo de material cifrado.	Elija un elemento.
7. Se ha comprobado el histórico de brechas de datos personales.	Elija un elemento.

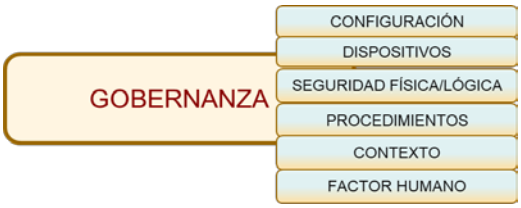
Vulnerabilidad en el receptor que afecta al emisor:

Robo de cookies y tokens de sesión en el receptor[73]

3.9 GOBERNANZA Y POLÍTICAS DE PROTECCIÓN DE DATOS

Más allá de la fortaleza teórica de un criptosistema, la seguridad real de un sistema de cifrado se deriva de la correcta aplicación de medidas de gobernanza y políticas, que en el caso que nos ocupa están centradas en la protección de datos.

La gobernanza de la información en la organización ha de ser una, y ha de integrar las políticas de protección de datos. Un tratamiento solo cumplirá con el principio de responsabilidad proactiva, o será "*accountable*" si también lo es cada una de las fases y medios que emplea. De esta forma, en la gobernanza de la información en la organización se han de reflejar los requisitos para que el sistema de cifrado sea "*accountable*" al menos desde el punto de vista de protección de datos.



3.9.1 Control de configuración de los componentes del sistema de cifrado.

La configuración de los componentes es el conjunto de parámetros que se pueden ajustar para determinar su funcionalidad.

Control	Validación
1. Los elementos del sistema criptográfico han de estar configurados adecuadamente antes de la puesta en producción del tratamiento en donde se utiliza el sistema de cifrado.	Elija un elemento.

[73] https://www.theverge.com/2023/3/24/23654996/linus-tech-tips-channel-hack-session-token-elon-musk-crypto-scam

2. La configuración de cada elemento está documentada.	Elija un elemento.
3. No se puede ejecutar el sistema de cifrado con configuraciones por defecto, o estas no existen.	Elija un elemento.
4. Las actualizaciones automáticas de cualquier elemento no alteran la configuración ni la reinician.	Elija un elemento.
5. Existe una política de control de acceso implementada y de registro de acceso a la configuración de cada elemento.	Elija un elemento.

Dispositivos móviles:

Existen patrones de ataque que consisten en la reinstalación de las librerías de cifrado con clave todo a ceros[74].

Bases de datos corporativas:

Una compleja arquitectura de cifrado de bases de datos puede verse comprometido por el acceso a las claves si no se configura el almacenamiento de estas adecuadamente[75].

3.9.2 Dispositivos

Dado que todos los elementos que configuran la suite de cifrado se ejecutarán sobre servidores, routers, ordenadores, tanto en sistemas personales o en entornos empresariales o corporativos, una inadecuada configuración puede comprometer la seguridad de todo el sistema criptográfico.

Control	Validación
1. Hay una política de seguridad y un control sobre los dispositivos BYOD que se emplean en el sistema de cifrado, o directamente no se permiten.	Elija un elemento.
2. Existe un control o la prohibición de instalar aplicaciones en dispositivos que ejecuten sistemas de cifrado sin autorización del responsable de seguridad.	Elija un elemento.
3. Se emplean versiones de los sistemas operativos especialmente configuradas para alta seguridad.	Elija un elemento.
4. Los dispositivos sobre los que se ejecute el sistema de cifrado están analizados ante vulnerabilidades específicas de los mismos.	Elija un elemento.
5. No se permite el uso de dispositivos que impida tener actualizado todo el sistema de cifrado.	Elija un elemento.
6. Los dispositivos del sistema de cifrado se utilizarán únicamente en entornos protegidos.	Elija un elemento.

[74] https://www.krackattacks.com/
[75] https://matthewmcgiffen.com/2018/01/03/how-secure-is-transparent-data-encryption-tde-and-how-to-prevent-hacking/

Dispositivos IoT, teléfonos VoIP y otros:

Muchos dispositivos no admiten configuraciones del tipo 802.1X al tener funciones muy limitadas, además suelen contar con pobres implementaciones de la criptografía y la gestión de contraseñas. El uso de otros mecanismos alternativos como MAC Authentication Bypass[76] que pueden no ser lo suficientemente seguros, pueden permitir que dispositivos externos accedan a las redes en donde se está usando el sistema criptográfico.

Los sistemas VoIP con vulnerabilidades o mal configurados pueden comprometer la red corporativa[77].

Sistemas de gestión de dispositivos móviles (MDM):

Los sistemas MDM han de estar convenientemente configurados para evitar que se puedan incorporar dispositivos externos no autorizados[78]. Son sistemas susceptibles de vulnerabilidades y han de mantenerse actualizados[79].

3.9.3 Seguridad física/lógica

Los sistemas, los dispositivos (más si son portátiles), los sistemas de backup, las pantallas, etc., pueden ser accesibles por terceros o directamente robados. El listado de controles mostrado a continuación se refiere a lo relativo al material de cifrado.

Control	Validación
1. Hay una política y establecimiento de áreas restringidas.	Elija un elemento.
2. Las políticas definen los dispositivos de almacenamiento permitidos.	Elija un elemento.
3. Existe un control de acceso físico y lógico autorizado a los dispositivos y material de cifrado, archivos de mensajes y claves, archivos temporales, procedimientos de cifrado.	Elija un elemento.
4. Existe un registro de acceso a los dispositivos y material de cifrado, archivos de mensajes y claves, archivos temporales, procedimientos de cifrado.	Elija un elemento.
5. Existe un listado de personal implicado en el proceso y de sus roles.	Elija un elemento.
6. Existe un protocolo de destrucción confidencial de todo el material relacionado con el sistema de cifrado.	Elija un elemento.
7. Existen medidas de prevención de ataques black-bag[80].	Elija un elemento.
8. No hay visualización directa de los elementos del sistema de cifrado.	Elija un elemento.
9. Todos los backup están controlados.	Elija un elemento.
10. No existe almacenamiento en terceros.	Elija un elemento.
11. Se han realizado análisis de memoria en caliente (Heartbleed SSL) o en	Elija un

[76] https://www.portnox.com/cybersecurity-101/mac-authentication-bypass/
[77] https://thehackernews.com/2023/03/critical-flaw-in-cisco-ip-phone-series.html
[78] https://book.hacktricks.xyz/macos-hardening/macos-security-and-privilege-escalation/macos-mdm/enrolling-devices-in-other-organisations
[79] https://www.securityweek.com/1000-organizations-exposed-remote-attacks-filewave-mdm-vulnerabilities/
[80] https://en.wikipedia.org/wiki/Black-bag_cryptanalysis

arranque en frío.	elemento.
12. Se ha buscado el uso de keyloggers y medidas para evitarlos.	Elija un elemento.
13. Existen medidas para evitar las manipulaciones de operaciones intermedias.	Elija un elemento.
14. Existen medidas de prevención de ataques Tempest.	Elija un elemento.

Robo o destrucción de dispositivos:

El acceso físico a los dispositivos que contienen información cifrada permite materializar ataques a la disponibilidad de la información, directamente por el robo o destrucción del soporte de los datos, además de facilitar la posible ruptura del sistema de cifrado y afectar a la confidencialidad.

Mecanismos de cifrado de discos:

Los sistemas de cifrado de disco protegen los datos cuando los equipos están apagados. En el caso de que el usuario haya entrado en el sistema y haya dejado el equipo está encendido, el sistema operativo ya se ha encargado de descifrar los datos sensibles y estarán disponibles para cualquiera que acceda al mismo.

Acceso físico al dispositivo:

Un acceso físico repetido puede aprovechar vulnerabilidades en sistemas criptográficos. LUKS tiene una funcionalidad de re-cifrado (reencprypt) con un fallo CVE-2021-4122, que reúsa un mecanismo para la operación de re-cifrado. Un atacante con acceso físico repetido puede simular un proceso de re-cifrado inacabado y conseguir el descifrado del dispositivo LUKS[81]

3.9.4 Gestión y Políticas

El RGPD exige en el art.5.2 un modelo de gobernanza con relación a los datos personales que sea "*accountable*", es decir, capaz de ser explicado y sometido a la transparencia, justificación y explicación de las acciones tomadas. Además, el art.24.2 establece la oportunidad de "Cuando sean proporcionadas en relación con las actividades de tratamiento, se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos".

Control	Validación
1. El sistema de cifrado se ajusta en su diseño, implementación y validación a las políticas y procedimientos establecidos por el responsable.	Elija un elemento.
2. Está documentado el ciclo de vida de los datos en el tratamiento (categoría de datos, flujo de los datos desde la incepción a la destrucción).	Elija un elemento.
3. Está documentada una evaluación de la fortaleza necesaria y de la calidad del sistema de cifrado en cada tratamiento en función del riesgo para los derechos y libertades fundamentales.	Elija un elemento.
4. Existe una unidad/persona (u/p) a cargo del sistema de cifrado.	Elija un elemento.
5. Dicha u/p mantiene una política adecuada y documentada del uso de cifrado	Elija un

[81] https://linuxiac.com/cryptsetup-vulnerability/

en el tratamiento con relación a todos los elementos y controles.	elemento.
6. Los tratamientos se categorizan por su necesaria fortaleza y se emplean distintas implementaciones y políticas adecuadas a dicha criticidad.	Elija un elemento.
7. La política recoge las recomendaciones del DPD o del asesor en protección de datos.	Elija un elemento.
8. Dicha política está sujeta al registro y ciclo de aprobación de los responsables de la entidad.	Elija un elemento.
9. Dicha política recoge el flujo/ciclo de vida de todos los componentes del inventario de la suite (se ha indicado anteriormente).	Elija un elemento.
10. Están identificados terceros/proveedores intervinientes (p.ej. validadores de certificados, SaaS, …).	Elija un elemento.
11. Están recogidos los contratos con terceros intervinientes.	Elija un elemento.
12. En los contratos con terceros, en la medida en que realizan cifrado de datos personales, se establecen instrucciones sobre el cifrado de datos, pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de los controles del criptosistema seleccionado por el responsable, así como mecanismos de supervisión y auditoría de los mismos.	Elija un elemento.
13. Está establecida una supervisión regular de los proveedores del sistema de cifrado (por ejemplo, con un 'vendor assessment').	Elija un elemento.
14. Dicha política recoge los requisitos de protección de datos establecidos por el DPD o la asesoría de protección de datos.	Elija un elemento.
15. Incluye la definición de roles (administrador, usuario), control de accesos, autenticación, procedimientos para usuarios, destrucción de material criptográfico, gestión de integridad, incidencias y avisos y planes de contingencia.	Elija un elemento.
16. En la política se establecen los plazos y eventos que desencadenan un proceso de validación, mantenimiento, baja de productos y/o auditoría.	Elija un elemento.
17. En la política se contemplan estrategias de re-cifrado de la información en reposo adecuadas al contexto técnico y de brechas de datos.	Elija un elemento.
18. La política recoge un procedimiento de auditoría y prueba de las actualizaciones de los elementos del sistema de cifrado.	Elija un elemento.
19. Las actualizaciones en procedimientos/hardware o software no se incorporan automáticamente a los sistemas en producción.	Elija un elemento.
20. Existe una política implementada de gestión de backup de la suite, la configuración y las claves.	Elija un elemento.
21. Existe una política de depósito de claves.	Elija un elemento.
22. Dicha política está integrada en la política de seguridad.	Elija un elemento.
23. La política no descansa exclusivamente en la automatización.	Elija un elemento.
24. El acceso a la política o sus partes está restringido siguiendo el principio de "need-to-know".	Elija un elemento.
25. En la política está establecido un proceso de identificados y evaluación continua de los cambios en la sensibilidad de la información cifrada, bien sea por cambios en las categorías de datos, categorías de sujetos, volumen de individuos afectados u otros.	Elija un elemento.
26. Existen canales de comunicación para incidencias sobre el proceso global de cifrado que llegan a esa unidad/persona.	Elija un elemento.

27. Existen canales para la comunicación interna y para las comunicaciones con fuentes del exterior.	Elija un elemento.
28. El delegado de protección de datos está incluido en todos los procedimientos de definición y validación del criptosistema.	Elija un elemento.
29. El administrador no puede realizar un bypass de los procedimientos de cifrado.	Elija un elemento.
30. Existen procedimientos para impedir transmitir información confidencial sin cifrar.	Elija un elemento.
31. Está procedimentado el proceso de recepción y atención de solicitudes por autoridades a material de cifra.	Elija un elemento.
32. Si la organización emplea canales ocultos en el sistema de cifrado para supervisión e inspección de contenido, la gestión está sometido a estrictos criterios de auditoría continua con implicación del DPD.	Elija un elemento.
33. Disponer de un plan de contingencia para el caso de que se detecte que el criptosistema puede estar comprometido.	Elija un elemento.
34. Existe un procedimiento para el cumplir con las obligaciones RGPD para el caso de que se detecte un compromiso del sistema de cifrado que afecte a datos personales.	Elija un elemento.

Empleado desaparecido:

Un empleado de la organización que es el único que conoce una clave desaparece. El empleado no ha seguido la política de depósito de las claves, o esta no existe o no está realmente funcionando en la organización. En ese caso, la organización no puede acceder a toda la información que ha sido previamente cifrada por dicho empleado.

Codificación:

Al actualizar una librería de cifrado reescribiendo C++ a Java, en la verificación ECDS se cometió un olvido al no contemplar los valores de R y S nulos, que es una vulnerabilidad que permite interceptar comunicaciones, falsificar certificados SSL, etc.[82]

Cifrado de documentos en reposo:

El compromiso de la clave maestra en una organización permitió el acceso por terceros a un número indeterminado de los pasaportes de clientes almacenados por una multinacional hotelera, se debió a una mala política de configuración, control, evaluación y gestión de claves[83].

3.9.5 Contexto y brechas de datos personales

El contexto es el conjunto de circunstancias que rodean a la organización, el tratamiento y el estado de la técnica. El contexto siempre cambia dinámicamente. Dentro de los cambios de contexto, un indicativo crítico son las brechas de datos personales que se producen con relación al sistema de cifrado en organizaciones, tratamientos o tipos de sistemas similares. Estos incidentes hay que detectarlos, analizarlos en el contexto del tratamiento y tomar las acciones oportunas para que no afecten a la propia organización.

[82] https://neilmadden.blog/2022/04/19/psychic-signatures-in-java/
[83] https://www.techtarget.com/searchsecurity/news/252455488/Marriott-data-breach-exposed-5-million-unencrypted-passport-numbers

Control	Validación
1. Existe una recopilación continua y un análisis de las brechas e incidencias que se producen con relación al sistema de cifrado en organizaciones, tratamientos o sistemas similares.	Elija un elemento.
2. Existe una recopilación continua y análisis de las nuevas vulnerabilidades conocidas que pueden afectar a todo el sistema de cifrado.	Elija un elemento.
3. Están identificados y se evalúan de forma continua los cambios en el marco jurídico que afectan a la entidad o al tratamiento e identificados los riesgos legales de futura normativa.	Elija un elemento.
4. Están identificados y se evalúan de forma continua los avances tecnológicos relativos al criptoanálisis, tanto los actuales como las estimaciones de cambio a medio plazo.	Elija un elemento.

Cambio del marco jurídico:

Con relación al marco jurídico, hay que tener en cuenta las posibles iniciativas normativas a nivel europeo que se están planteado para permitir el acceso a autoridades públicas a comunicaciones cifradas[84].

Puertas traseras en componentes certificados:

En algunos casos, los propios organismos de estandarización promueven componentes en los que se incluyen puertas traseras conocidas por un círculo reducido[85]. Uno de los casos más conocido implicaba un componente de la suite (generador de números aleatorios[86]) certificado por el NIST.

3.9.6 Factor humano

El elemento humano es el factor más importante en cualquier sistema de seguridad y a veces se le dedica una menor atención. En particular, las brechas que se originan por una acción u omisión de los intervinientes humanos pueden provocar los mayores impactos en un tratamiento.

Control	Validación
1. Existen procedimientos escritos disponibles para el personal que maneja material de cifrado.	Elija un elemento.
2. El personal está obligado a firmar compromisos de confidencialidad en los que se les informa de sus obligaciones y las responsabilidades a las que debe hacer frente.	Elija un elemento.
3. El personal está formado para ejecutar los procedimientos que les compete.	Elija un elemento.
4. Existen planes de formación continua sobre los procedimientos.	Elija un elemento.
5. Existe formación y procedimientos específicos orientados a detectar la existencia y catalogación de ataques de ingeniería social, así como posibles extorsiones o coacciones.	Elija un elemento.

[84] https://appleinsider.com/articles/22/05/11/eu-plans-to-require-backdoor-to-encrypted-messages-for-child-protection
[85] https://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220
[86] https://en.wikipedia.org/wiki/Dual_EC_DRBG#Software_and_hardware_which_contained_the_possible_backdoor

6.	Existe supervisión de la ejecución manual de los procedimientos.	Elija un elemento.
7.	Existe un procedimiento interno de sanción para el no seguimiento de los procedimientos de cifrado.	Elija un elemento.
8.	En los procesos de selección de personal interno/externo para puestos a cargo de las operaciones más críticas, se ha de superar un proceso de examen y la revisión de los antecedentes.	Elija un elemento.
9.	El personal a cargo de las operaciones más críticas pasa de forma regular por un proceso de reevaluación técnica y de confiabilidad.	Elija un elemento.

Acceso a acreditaciones:

Recientemente se publicó en un canal de Telegram un anuncio en el que se ofrecía un pago a través de la Darkweb, no por datos, sino por credenciales de acceso a sistemas informáticos. Este tipo de ataques cada vez son más frecuentes ya que permiten acceder al corazón de la entidad.

4 CONCLUSIÓN

Como establece el artículo 32 en su apartado 1.b, el sistema de cifrado, como todos los elementos de seguridad en su conjunto, deben ser verificados, evaluados y valorados regularmente con relación a su eficacia en la protección de los derechos y libertades de las personas, entre otros. Esta es una obligación de responsables y encargados/subencargados, y el DPD o, en su defecto, los asesores en protección de datos han de estar involucrados en el asesoramiento y en la supervisión del proceso regular de verificación, evaluación y valoración del sistema de cifrado.

Un sistema de cifrado es una operación compleja que se incluye en muchos tratamientos y que no se puede abordar de forma superficial. Cuando el sistema de cifrado se compromete en un tratamiento de datos personales, se materializan unos riesgos para los derechos y libertades que serán específicos para cada tratamiento. Para la determinación de dichos riesgos es necesario, además de determinar qué datos se han comprometido, evaluar el impacto que el compromiso de esos datos puede producir en los individuos afectados y en la sociedad. La fortaleza y robustez del sistema de cifrado ha de estar dimensionado ha dicho impacto.

Teniendo en cuenta que ningún sistema de seguridad incorpora una garantía de infalibilidad, el responsable no debe limitar las medidas para gestionar los riesgos para los derechos y libertades a las medidas de seguridad, en particular, hacer descansar toda la gestión del riesgo únicamente en el cifrado de la información. El responsable ha de incorporar, desde el propio concepto del tratamiento, medidas de privacidad para minimizar los impactos derivados de una posible materialización de una brecha de datos personales, tales como políticas para la protección de datos, privacidad por defecto y diseño (minimización, anonimización temprana, seudonimización, cancelación de datos, agregación, baja granularidad, transparencia, etc.), mecanismos de gobernanza y de gestión de brechas de datos personales mediante la elaboración y ejecución de planes de contingencia, entre otros.

5 REFERENCIAS

- 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).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE Versión 2.0
- AEPD: Cifrado y Privacidad: cifrado en el RGPD
- AEPD: Cifrado y Privacidad II: El tiempo de vida del dato [ene 2020]
- AEPD: Cifrado y Privacidad (V): la clave como dato personal [dic 2021]
- ISO 27002/2022
- CCN Criptología de empleo en el Esquema Nacional de Seguridad
- CCN Taxonomía de productos STICAnexoE.1: Dispositivos de almacenamiento cifrado
- CCN Taxonomía de referencia para productos de seguridad TIC - Anexo E.2: Dispositivos/Herramientas de cifrado offline
- ENISA: Study on cryptographic protocols
- ENISA: Algorithms, key size and parameters report 2014
- ENISA: Data protection Engineering 2022
- NIST: Cryptographic Standards and Guidelines

6 ANEXOS

6.1 ANEXO: SISTEMAS DE CLAVE SIMÉTRICA, ASIMÉTRICA Y MIXTOS

6.1.1 Cifrado simétrico

Los esquemas para el cifrado simétrico parten de la hipótesis de que los usuarios involucrados en la comunicación comparten una clave secreta (completamente impredecible para un adversario). Fundamentalmente, se utilizan dos tipos de esquemas:

6.1.1.1 Cifrado en bloque. Modos de operación

Un cifrador en bloque procesa bloques de información de tamaño fijo (típicamente 128 o 256 bits) que se cifran o descifran con claves de tamaño similar. En la actualidad, el cifrador en bloque más recomendado es el AES, estandarizado por el NIST en 2001. El tamaño mínimo de bloque (y clave) recomendado son 128 bits.

Tan relevante como elegir un cifrador en bloque adecuado es implementar un modo de operación que dicte cómo manipular conjuntos de datos de más de un bloque. Los más recomendados son los modos CCM y GCM (ver. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38c.pdf y https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38d.pdf).

6.1.1.2 Cifrado en flujo.

Un cifrador en flujo es habitualmente apropiado para el cifrado dinámico de datos (por ejemplo, transmitidos por streaming). Cuando el cifrador en bloque AES se usa en modo CTR el resultado es un cifrador de este tipo.

6.1.2 Cifrado asimétrico

Los esquemas de cifrado asimétrico se caracterizan por existir una división del material de clave, de modo que sólo el receptor dispone de una clave secreta, poniendo a disposición pública su llamada clave pública para que sea accesible a cualquier emisor. Los esquemas simétricos más utilizados hasta la fecha son el cifrado RSA (en concreto, la llamada variante RSA-OAEP) y aquellos que utilizan como base el problema del logaritmo discreto, frecuentemente en grupos asociados a curvas elípticas (El Gamal). Para seguridad a largo plazo es necesario buscar otras alternativas, pues estos esquemas son vulnerables a ataques cuánticos (ver 2.1.6.)

6.1.3 Funciones hash

Las funciones hash o funciones resumen son piezas fundamentales de muchos esquemas criptográficos, además de usarse aisladamente para proporcionar pruebas de integridad. Así, es frecuente que la transmisión de un documento X (cifrado o no) se complete con el envío de un resumen H(X), siendo H una función criptográfica que permite, hasta cierto punto, detectar modificaciones (intencionales o no) sobre el texto X que hayan podido producirse en tránsito. Las funciones hash actualmente más recomendadas pertenecen a la llamada familia SHA; por ejemplo, SHA-256, SHA-512/256, SHA3-256, SHA3-515. El sufijo numérico indica el número de bits de salida, es decir, el tamaño del resumen del documento (que es fijo, no depende del tamaño del documento de entrada).

6.1.4 Mecanismos para Establecimiento de Clave

El establecimiento de claves criptográficas (para su uso posterior en escenarios simétricos) puede hacerse a través de mecanismos tanto simétricos como asimétricos. Habitualmente, de hecho, se consideran mecanismos criptográficos mixtos en los que tras

intercambiar una clave criptográfica usando un mecanismo asimétrico (como Diffie-Hellman o EC Diffie-Hellman) esta clave se utiliza para cifrar con un cifrador en bloque (como AES).

Si el establecimiento de clave quiere hacerse por medios simétricos también es posible (ver ISO/IEC 11770-2:2018).

6.1.5 Autenticación

Autenticación supone verificar la identidad de aquellos que se comunican con nosotros, o el origen de un mensaje o bloque de datos es crucial a la hora de complementar las garantías que proporciona el cifrado. Existen diferentes mecanismos para este fin,

6.1.5.1 Contraseñas

Son un mecanismo relativamente débil de autenticación, que ha de implementarse exclusivamente al amparo de mecanismos que limiten el número de peticiones de acceso (para evitar ataques de diccionario). Es importante no almacenar contraseñas en claro ni resumidas a través de un hash, para evitar filtrado de datos de acceso.

6.1.5.2 Firmas

El uso de esquemas de firma digital es siempre la mejor manera de autenticar la comunicación, si bien es importante disponer de una gestión sólida de claves y certificados. Los mecanismos de firma más recomendado son firmas basadas en RSA, firmas basadas en logaritmo discreto (DSA y sus variantes sobre curvas elípticas ECDSA, ECKDSA), además de las firmas de Merkle (XMSS+ o LMS) – siendo estas últimas preferibles a largo plazo. Las firmas RSA y DSA son vulnerables a ataques cuánticos, por lo que para aplicaciones a largo plazo se recomienda utilizar herramientas post-cuánticas.

6.1.5.3 MACs

Los códigos de autenticación de mensajes (MACs) sirven para generar etiquetas que permitan la autenticación de datos en el escenario simétrico (tanto para la generación como para la verificación de la etiqueta se necesitará la misma clave simétrica). Los MACs suelen construirse a partir de cifradores en bloque o funciones hash. Ejemplos prominentes son CMAC, HMAC o GMAC, siempre con la recomendación de que las etiquetas generadas sean de al menos 96 bits y las claves asociadas de, al menos, 128 bits

6.1.6 Escenario Post-Cuántico

Desde 2017 la oficina de tecnología y estándares norteamericana (NIST) ha establecido un proceso internacional de selección de algoritmos criptográficos susceptibles de resistir ataques cuánticos. Dicho proceso se centra en mecanismos para encapsulado de clave (llamados KEM), y esquemas de firma digital. Los KEMs tienen la particularidad de adaptarse para dar lugar a esquemas de cifrado asimétrico y a esquemas de intercambio de clave, por lo que disponer de KEMs seguros proporciona una colección de herramientas completa para los usos básicos en criptografía. En julio de 2022 se han señalado los primeros esquemas que se estandarizarán; el KEM CRYSTALS-Kyber (basado en retículos) y las firmas CRYSTALS-Dilithium y FALCON (también basadas en retículos), así como la firma SPHINCS+, que se construye a partir de funciones hash.

Muchos organismos internacionales están elaborando guías para facilitar la transición al mundo post-cuántico, es decir, la sustitución de criptografía basada en logaritmo discreto y factorización por herramientas fundamentadas en otros problemas matemáticos, como problemas de decodificación o relacionados con retículos. Ver, por ejemplo, la guía recientemente publicada en Europa por ETSI https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf.

6.2 ANEXO: LONGITUD DE LA CLAVE

Cuando se define la fortaleza de una clave por su longitud en bits hay que tener en cuenta que en cifrado asimétrico son unos tamaños y en cifrado simétrico son otros muy diferentes (Se mueven en rangos diferentes. AES es el estándar para cifrado simétrico del NIST y emplea claves de 128 bits, y claves de longitud 128, 192 o 256 bits (este sería, de hecho, el tamaño mínimo recomendado para resistir ataques cuánticos, en un horizonte de medio-largo plazo). Los algoritmos asimétricos emplean claves más largas de 1024 bits, 2048 o 3072 bits.

En 2003 RSA declaró que su clave de 1024 bits es equivalente a una clave simétrica de 80 bits. Su clave de 2048 bits es equivalente a una clave simétrica de 112 bits, y la clave de 3072 bits es equivalente a una clave de 128 bits. RSA recomienda usar al menos claves de 1024 bits si desea mantener sus documentos seguros hasta 2010, y usar una clave de 2048 bits si desea que los documentos estén seguros hasta 2030. La clave a 3072 se indica para los documentos que deben permanecer seguros después de 2030. Un documento NIST define que una clave asimétrica de 15360 bits es equivalente a una clave simétrica de 256 bits en entornos post-cuánticos, si bien en el medio/largo plazo se aconseja utilizar otros métodos de cifrado más resistentes a los ataques cuánticos conocidos.

Los tamaños de clave recomendados para herramientas post-cuánticas pueden, por ejemplo, consultarse en el reciente informe del NIST https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf . Por ejemplo, los tamaños de clave para cifrar con CRYSTALS-Kyber recomendados oscilan entre 800 y 1568 bits para la clave pública, duplicando (aproximadamente) estos tamaños las claves secretas correspondientes.

6.3 ANEXO: CONSEJOS CON RELACIÓN A UN SISTEMA DE CIFRADO

El cifrado es una herramienta muy poderosa para proteger los datos. El cifrado como medida de garantía para reducir o mitigar el riesgo en un tratamiento de datos personales solo será efectivo si su uso es adecuado y correcto. En caso contrario, se vuelve inútil si el dispositivo, procedimientos, protocolos o personas involucrados en su operación se ven comprometidos.

La criptografía tiende a fallar en su aplicación práctica más que en errores en el algoritmo teórico. Los sistemas de cifrado en el mundo real se implementan sobre múltiples productos hardware y software, combinando primitivas y herramientas, lo que puede presentar riesgos. Pero aun existiendo buenos algoritmos y protocolos para la mayoría de los casos, los errores al configurar y validar la utilización del sistema de cifrado son la fuente de la mayoría de las vulnerabilidades.

Algunos errores frecuentes que es preciso evitar son[87]:

- No emplear especialistas en criptografía y en protección de datos para definir un criptosistema para proteger datos personales.
- Confiar en las herramientas, servicios, soporte de terceros o en tu propio personal sin las apropiadas validaciones regulares.
- No formar a empleados.
- No validar el criptosistema que depende de encargados, proveedores y terceros.
- No adecuar la fortaleza del criptosistema al impacto real que puede producir una brecha en el mismo.
- Cifrar información que no es necesario cifrar.

[87] https://crashtest-security.com/owasp-cryptographic-failures/

- Crear tu propio algoritmo u otros elementos de la suite de cifrado.
- Utilizar configuraciones por defecto.
- Hacer un despliegue no validado de actualizaciones.
- Realizar una incorrecta protección y/o gestión de claves criptográficas.
- Reutilizar elementos para implementar parte del sistema de cifrado.
- Utilizar canales que eviten usar la criptografía por “comodidad”.
- No emplear métodos superpuestos de protección: cifrado-cifrado, esteganografía-cifrado, cifrado-líneas dedicadas, etc.
- No emplear en comunicaciones sistemas de cifrado autenticado.
- Emplear aleatoriedad que no contempla los requisitos para un sistema criptográfico.
- Faltar al principio “*need to know*” con relación al criptosistema.
- No implementar un ciclo de vida de la gestión de claves.
- Distribuir la información o las claves en algún momento en texto claro,
- Primar la funcionalidad sobre la seguridad.

El consejo final es realizar auditorías periódicas de los procedimientos y del uso del material criptográfico, que incluya preparar periódicamente “trampas” para determinar si se está siendo monitorizado, si nuestros propios usuarios no siguen los procedimientos y si el sistema es suficientemente fuerte (hacking ético).

7 TABLA DE ACRÓNIMOS

AEPD. Agencia Española de Protección de Datos
AES. Advanced Encryption Standard
APEP. Asociación Profesional Española de Privacidad
BYOD. Bring Your Own Device
CCM. CBC Counter Mode
CMAC. Cipher-based Message Authentication Code
CTR. Counter
DES. Data Encryption Standard
DPD. Delegado de protección de datos
DSA. Digital Signature Algorithm
EC Diffie-Hellman. Elliptic-curve Diffie-Hellman
ECB. Electronic Code Book
ECDSA. Elliptic Curve Digital Signature Algorithm
ECKDSA. Korean version of ECDSA
ENS. Esquema Nacional de Seguridad
GCM. Galois/Counter Mode
GMAC. Galois Message Authentication Code
HMAC. Hash-based Message Authentication Code
HNLD. Harvest Now, Decrypt Later
HSM. Hardware Security Module
HW/SW. Hardware/Software
IoT. Internet of Things
ISMS Forum. Asociación Española para el Fomento de la Seguridad de la Información
JWE. JSON Web Encryption
JWT. JSON Web Token
KEM. Key-encapsulation Mechanism
LMS. Leighton-Micali Signature
LUKS. Linux Unified Key Setup
MAC. Message Authentication Code
MD5. Message Digest Algorithm 5
MDM. Mobile Device Management
MITM. Man In The Middle
NIST. National Institute of Standards and Technology
OAEP. Optimal Assymetric Encryption Padding

OWASP. Open Worldwide Application Security Project
PBKDF2. Password-Based Key Derivation Function 2
PEC. Privacy Enhancing Crytography
PET. Privacy Enhancing Technologies
PIR. Private Information Retrieval
PKCS. Public-Key Cryptography Standards
PMKID. Pairwise Master Key Identifier
POODLE. Padding Oracle On Downgraded Legacy Encryption
PSI. Private Set Intersection
RGPD. Reglamento General de Protección de Datos
RSA. Rivest-Shamir-Adleman
RTU. Remote Terminal Unit
SaaS. Software as a Service
SHA. Secure Hash Algorithm
SNLD. Store Now, Decrypt Later
SSE. Searchable Symmetric Encryption
SSH. Secure Shell
SSL. Secure Sockets Layer
StE. Structured Encryption
TIC. Tecnologías de la Información y las Comunicaciones
TLS. Transport Layer Security
VoIP. Voice over Internet Protocol
WEP. Wired Equivalent Privacy
WPA. Wi-Fi Protected Access
XMSS. eXtended Merkle Signature Scheme
ZKPoK. Zero-Knowledge Proofs of Knowledge