Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de proyecto de investigación aplicada 2

Tema:

Propuesta de modelo de selección de algoritmos criptográficos modernos simétricos y asimétricos incluyendo curvas elípticas aprobadas para entornos informáticos

Elaborado por:

Gutiérrez Ruiz Alexander Daniel

Diciembre, 2022

Declaratoria de derechos de autor

Se declara que la presente investigación ha sido realizada por el autor único Alexander Daniel Gutiérrez Ruiz y, a su vez, se ha utilizado diversas fuentes bibliográficas con sus respectivas referencias bibliográficas y citaciones en los distintos capítulos que se presentan en la investigación, de esta manera, respetando completamente los derechos de autor de sus respectivos creadores. También, se ha hecho uso de diversos datos recopilados a través de encuestas cuyo objetivo es poder evidenciar los datos expertos o del público meta.

Se autoriza el uso parcial o total de la presente investigación para ser empleada como referencia de futuros trabajos de investigación ya sean académicos o científicos teniendo la condición de que sea referenciado de manera adecuada en las referencias.

Agradecimiento

En primer lugar, agradezco a Dios, por darme salud, fuerza y sabiduría para hacer posible este trabajo incluso desde antes de haberlo iniciado.

Además, quiero agradecer el apoyo incondicional de mi novia, Vanessa Romero Rivera, quien ha estado presente en todo momento, tanto en el desarrollo de mi vida personal como la profesional.

A la Universidad Cenfotec y a sus profesores, cuyos conocimientos compartidos son base para elaborar la presente investigación, en especial a Luis Alfonso Ramírez Jiménez y Dennis Alonso Durán Céspedes, quienes a través de sus mentorías, proceso formativo y orientación han sido vitales para este proceso, lo cual me ha permitido desarrollar este proyecto de manera asertiva y exitosa.

Aprobación del Tribunal

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Gutiérrez Ruiz Alexander Daniel.**

DENNIS ALONSO DURAN CESPEDES (FIRMA)
Firmado digitalmente por DENNIS ALONSO DURAN CESPEDES (FIRMA)
Fecha: 2023.03.13 18:45:37 -06'00'

M.Sc. Dennis Alonso Durán Céspedes
Tutor

JOSE DAVID IBARRA QUESADA (FIRMA)
Firmado digitalmente por JOSE DAVID IBARRA QUESADA (FIRMA)
Fecha: 2023.03.13 18:59:26 -06'00'

M.Sc. José David Ibarra Quesada
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA)
Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA)
Fecha: 2023.03.13 20:35:42 -06'00'

M.Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 13 de marzo de 2023

Carta de aprobación del filólogo

Cartago, 10 de marzo de 2023

Los suscritos, Elena Redondo Camacho, mayor, casada, filóloga, incorporada a la Asociación Costarricense de Filólogos con el número de carné 0247, portadora de la cédula de identidad número 3-0447-0799 y, Daniel González Monge, mayor, casado, filólogo, incorporado a la Asociación Costarricense de Filólogos con el número de carné 0245, portador de la cédula de identidad número 1-1345-0416, ambos vecinos de Quebradilla de Cartago, revisamos el trabajo final de graduación que se titula: *Propuesta de modelo de selección de algoritmos criptográficos modernos simétricos y asimétricos incluyendo curvas elípticas aprobadas para entornos informáticos*, sustentado por Gutiérrez Ruiz Alexander Daniel.

Hacemos constar que se corrigieron aspectos de ortografía, redacción, estilo y otros vicios del lenguaje que se pudieron trasladar al texto. A pesar de esto, la originalidad y la validez del contenido son responsabilidad directa de la persona autora.

Esperamos que nuestra participación satisfaga los requerimientos de la Universidad Cenfotec.

X ANA ELENA REDONDO CAMACHO (FIRMA)
Firmado digitalmente por ANA ELENA REDONDO CAMACHO (FIRMA)
Fecha: 2023.03.10 10:46:24 -06'00'

Elena Redondo Camacho
Filóloga - Carné ACFIL n.º 0247

X DANIEL ALBERTO GONZALEZ MONGE (FIRMA)
Firmado digitalmente por DANIEL ALBERTO GONZALEZ MONGE (FIRMA)
Fecha: 2023.03.10 10:45:54 -06'00'

Daniel González Monge
Filólogo - Carné ACFIL n.º 0245

Índice de tablas

ÍNDICE DE FIGURAS

Resumen

La encriptación en el ámbito informático existe desde hace muchos años y sus usos son tan variados como sus posibilidades lo permitan en las diferentes áreas de la informática moderna. Sin embargo, un gran porcentaje de informáticos posee poco o nulo conocimiento sobre la criptografía y, por lo tanto, su aplicabilidad para proteger los datos en sus diferentes estados. Lo anterior permite que existan brechas, las cuales propician la degeneración de la seguridad sobre los datos en la confidencialidad, integridad y disponibilidad.

Por lo tanto, es de gran relevancia en el ámbito actual proporcionar la información y la forma de selección criptográfica óptima para agregar mayor seguridad a los datos y, por ende, a la información de las organizaciones. Lo anterior debe hacerse de una manera asimilable que propicie su uso en un mundo tan globalizado, digitalizado y peligroso como es el actual.

Palabras clave: seguridad informática, algoritmo criptográfico, aplicabilidad, moderno, simétrico, asimétrico, curva elíptica.

Capítulo 1. Introducción

1.1 Generalidades

En la actualidad, los algoritmos criptográficos que se utilizan en la industria informática tienen su contenido y conformación de forma gratuita y de fácil acceso para el público en general. El presente trabajo usa este contenido con el fin investigativo.

1.2 Antecedentes del problema

En los últimos años, los ataques informáticos a distintas empresas y entidades gubernamentales y privadas han aumentado exponencialmente debido a la gran expansión del Internet y los servicios que se brindan. Esto implica manipular y transmitir información por diversos medios computacionales, lo cual acrecienta el área de ataque para los ciberdelincuentes, lo que implica daños millonarios como lo menciona Procomer de Costa Rica (2022) con base en el estudio realizado por IBM y presentado a través del informe X-Force Threat Intelligence Index 2022.

Es importante mencionar que este informe expone el incremento y la complejidad de los ataques para infiltrarse y robar la información de las empresas y tiene a los *ransomware* como el tipo de ataque más letal para las organizaciones. Por este motivo, es necesaria la implementación de la criptografía en los sistemas informáticos de forma acertada para el medio en donde se encuentren los datos, con el fin de mitigar su robo.

1.3 Definición y descripción del problema

El presente trabajo tiene como objetivo evaluar la selección acertada de la criptografía moderna en entornos informáticos a través del análisis, comparación y evaluación de los algoritmos simétricos y asimétricos incluyendo curvas elípticas seguras.

Se debe señalar que la evaluación y comparación de los algoritmos criptográficos se aborda con el objetivo de simplificar su utilización y, de esta manera, su elegibilidad para su uso en distintos ámbitos de la informática de forma segura y acertada para los objetivos destinados. Como menciona Molinero Gil (2018), la privacidad y anonimidad de la información dentro de una red es un gran problema actual, debido a la cantidad masiva de datos que se transmiten. Esto genera problemas de diversas índoles por el aumento y complejidad de ataques cibernéticos.

1.4 Justificación

El motivo principal por el cual se desea desarrollar un modelo de selección de algoritmos criptográficos modernos para las distintas áreas de la informática es para promover su uso en las actividades diarias y fortalecer la integridad de los datos. A la vez, realizar recomendaciones sobre la aplicabilidad de cada algoritmo en los distintos entornos en donde se encuentren los datos.

Adicionalmente, se espera que este proyecto sirva como referencia para que cualquier persona con conocimientos informáticos pueda elegir el algoritmo de encriptación más adecuado para las actividades que requiera. Esto con el fin de que no se divulgue información personal o empresarial, lo cual produciría impactos negativos, según la sensibilidad de la información.

1.5 Viabilidad

Con base en lo anterior, existe mucha documentación alrededor del tema sobre la criptografía. Sin embargo, esta documentación se enfoca en diversos temas, como en la forma en la que los algoritmos realizan los cifrados/descifrados de datos a nivel matemático y no sobre la selección de algoritmos criptográficos que se adecúen para los distintos entornos y tareas generales dentro de una organización de manera ordenada y concisa.

A continuación, se desarrolla el punto de vista técnico, operativo y económico, por los cuales se considera la factibilidad de la presente investigación.

1.5.1 Punto de vista técnico.

Como licenciado en Ciencias de la Computación, desarrollador sénior y futuro máster en Ciberseguridad, el autor cuenta con el conocimiento y experiencia en la evaluación e implementación de algoritmos criptográficos en diferentes ámbitos informáticos. De igual manera, se espera que, como parte del proceso evolutivo, se obtenga la experiencia a través de múltiples autores para abordar el problema que se planteó.

1.5.2 Punto de vista operativo.

Al tratarse de una investigación con enfoque en criptografía moderna a través de artículos y documentos existentes y gratuitos, no altera de ninguna forma el funcionamiento de los recursos que se utilizan.

1.5.3 Punto de vista económico.

Debido a que esta investigación tiene como propósito ofrecer resultados a los profesionales informáticos, el costo relacionado con el proyecto de horas de investigación, licencias de *software*, *hardware* y otros gastos concernientes corren por cuenta del autor del proyecto.

Al considerar los datos que brinda Deloitte (2022) en su IV edición de la encuesta salarial del sector de tecnologías de información 2020-2021, desde la cual se estima el sueldo mensual de los profesionales a partir de múltiples factores, se toma el rango del grupo de cargo en el ámbito de líder de equipo y de la columna “C.T (Compensación Total)” como se muestra a continuación:

Grupo de Cargos	S.B	O.R.G	T.G	R.V	C.T
Soporte	819,827	170,443	990,270	51,602	1,021,570
Profesional	1,377,500	211,090	1,588,591	145,398	1,669,424
Líder de equipo / supervisor	1,996,886	261,616	2,258,502	271,964	2,417,835
Gerencia	2,757,064	458,224	3,215,288	661,043	3,661,707

Figura 1: Salario mensual por cargos

Fuente: Elaboración basada en los datos de Deloitte (2022).

Salario			
Anual	Mensual	Diario	Hora
₡30.324.480	₡2.527.000	₡126.350	₡15.794

Tabla 1: Desglose de salario

Fuente: Elaboración basada en los datos de Deloitte (2022).

Horas de investigación			
Semanal	Duración TFG (Meses)	Duración TFG (Horas)	Costo estimado por consultor (hora)
30	4	480	₡15.794
		Total	**₡7.581.120**

Tabla 2: Costo de horas consultor

Fuente: Elaboración basada en los datos de Deloitte (2022).

1.6 Objetivos

Los siguientes objetivos se basan en la taxonomía de Benjamín Bloom.

1.6.1 Objetivo general.

Proponer un modelo de selección de algoritmos criptográficos modernos simétricos y asimétricos incluyendo curvas elípticas aprobadas para entornos informáticos.

1.6.2 Objetivos específicos.

1. Identificar los algoritmos criptográficos modernos simétricos y asimétricos incluyendo curvas elípticas actualmente aprobados que puedan implementarse en entornos informáticos, mediante un estudio comparativo.
2. Explicar los algoritmos criptográficos modernos simétricos y asimétricos incluyendo curvas elípticas actualmente aprobados con su eficiencia de implementación, a través de un informe investigativo.
3. Elaborar un análisis criptográfico que permita la visualización de las distintas ventajas y su impacto, mediante un informe de análisis de eficacia.
4. Identificar los entornos informáticos adecuados para la implementación de la criptografía, por medio de un informe investigativo.
5. Recomendar buenas prácticas de selección e implementación de criptografía en los distintos entornos informáticos, por medio de reportes.
6. Diseñar un modelo de selección de algoritmos criptográficos modernos simétricos y asimétricos incluyendo curvas elípticas aprobados para entornos informáticos, mediante un informe técnico.

1.7 Alcances y limitaciones

1.7.1 Alcances.

El proyecto tiene como alcance la propuesta de un modelo de selección de algoritmos criptográficos simétricos y asimétricos incluyendo curvas elípticas, además de buenas prácticas para el aprovechamiento de cada algoritmo en los distintos entornos informáticos. Se proponen técnicas de evaluación y elección de los algoritmos que se adapten a los entornos informáticos.

Además, el proyecto no pretende dar un proceso paso a paso de implementación ni ser un análisis profundo en temas matemáticos, sino una guía de buenas recomendaciones para seleccionar los algoritmos y llaves criptográficas para los distintos sistemas informáticos. De esa manera, aprovechar y dar mayor visibilidad a la importancia de mantener los datos seguros y anónimos en todo momento.

1.7.2 Limitaciones.

1. Se limita el estudio de algoritmos criptográficos modernos simétricos y asimétricos incluyendo curvas elípticas aprobados actualmente más populares y de uso público.
2. El proyecto no incluye el diseño de material de capacitación o de implementación de algoritmos en lenguajes de programación.
3. Las recomendaciones se dan de manera generalizada y pueden aplicarse en cualquier ambiente con capacidad de cómputo para gestionar criptografía.
4. Las pruebas se limitan al poder de cómputo con que cuente el equipo del autor.
5. Se cuenta con un único miembro para la realización del proyecto.
6. El proyecto está dirigido a la selección de algoritmos y llaves criptográficas.
7. El proyecto no propone la implementación explícita en ningún ambiente en específico.
8. Para el desarrollo del modelo se cuenta con el tiempo establecido por el tutor asignado por parte de la universidad. En cualquier circunstancia, la extensión de esta es notificada debidamente por parte del estudiante y con la justificación para la universidad.

1.8 Revisión de literatura

En esta sección se valida por medio de fuentes y documentos técnicos que informen y refuercen la necesidad de implementar la criptografía como parte cotidiana en el mundo digital.

1.8.1 Revisión sistemática

A continuación, se presentan las principales fuentes que respaldan el presente proyecto.

1.8.1.1 A Primer on Cryptography in Communications

Introducción a la criptografía simétrica y asimétrica incluyendo curvas elípticas en las comunicaciones computacionales:

1.8.1.2 Evaluación fuente

A continuación, se muestra la influencia de la fuente en el ámbito de las comunicaciones informáticas de acuerdo con SCImago Journal Rank:

Parámetro	Criterio	Valor Actual	Cumple
H-INDEX	> 29	19	No
Cuartiles	Verdes	Verdes	Si
SJR	>= 0.2	1.057	Si
Citación por documento	>= 0.4	1.33	Si

1.8.1.2 Estado de la cuestión

Existen esfuerzos en el ámbito nacional e internacional para introducir la criptografía en entornos informáticos para proteger la confidencialidad, disponibilidad e integridad de los datos en entornos informáticos. Se desea realizar una compilación de documentos técnicos, los cuales permitan el desarrollo del presente estudio y, de esa manera, llevar a cabo la identificación, selección y análisis.

1.8.2 Formulación de la pregunta

La formulación de la pregunta permite delimitar el esfuerzo en cuanto a la búsqueda de la información e investigación. El objetivo principal es encontrar las respuestas adecuadas para demostrar el aporte del trabajo al campo de la investigación y, a la vez, relacionarlo con ideas concernientes a la teoría y aplicación práctica.

1.8.2.1 Foco de la pregunta

Para la presente investigación se requiere centralizar la búsqueda de documentos técnicos que especifiquen el uso de algoritmos de encriptación modernos

simétricos y asimétricos incluyendo curvas elípticas en conjunto y, a la vez, validar su eficacia y rendimiento en el momento de cifrar y descifrar la información.

1.8.2.2 Calidad y amplitud de la pregunta

En este apartado se establece la pregunta de la investigación, la cual se desea evacuar de manera clara y directa con base en el problema por resolver. A continuación, se brinda un listado con términos clave con el objetivo de realizar la búsqueda de la información para determinar temas como la población específica, exposición y eventos de interés.

1.8.2 Problema

La complejidad de la criptografía y sus términos entre los sistemas informáticos ocasiona una curva bastante elevada para aquellos que poseen poco o nulo conocimiento sobre ciberseguridad, lo cual se traduce en implementaciones pobres para las necesidades que se tienen. El impacto de las malas o nulas implementaciones criptográficas puede llegar a grandes dimensiones donde se comprometa información de empresas e incluso gobiernos debido al aumento de ataques realizados por ciberdelincuentes con el paso de los años. Por lo tanto, realizar un modelo de selección de algoritmos criptográficos modernos aprobados actualmente tomó gran relevancia con el paso del tiempo. La presente investigación tiene el enfoque que se basa en estudios y artículos científicos en cuanto aplicación de criptografía moderna en entornos informáticos se refiere.

1.8.2.1 Pregunta

¿Cuáles trabajos se realizan en el área de la criptografía para su aplicación en sistemas informáticos?

1.8.2.2 Palabras clave y sinónimos

A continuación, se presenta un listado de palabras clave y sinónimos que se utilizan para localizar fuentes de información que se relacionan con el estudio. Como nota, algunas palabras se escriben en inglés debido al uso extendido de estos términos en el área de la informática y, por lo tanto, en las publicaciones que se puedan encontrar en este idioma.

Palabra clave	Equivalencia en inglés
Algoritmo	Algorithm
Criptografía	Cryptography
Entorno informático	IT environment
Técnicas	Techniques
Implementación	Implementation
Simétrico	Symmetric
Asimétrico	Asymmetric
Curvas elípticas	Elliptic curves
Moderno	Modern
No vulnerado	No vulnerable
Aplicabilidad	Applicability

Tabla 3: Listado de palabras

1.8.2.3 Intervención

Ver los resultados sobre cómo la aplicación de algoritmos criptográficos ayuda al fortalecimiento de la confidencialidad, disponibilidad e integridad de los datos en los entornos informáticos.

Extraer los documentos y artículos que impacten en mayor medida la investigación y el análisis de los resultados.

1.8.2.4 Control

Al inicio del estudio no se cuenta con ninguna base de información, por lo tanto, se inicia una búsqueda desde cero con base en las palabras clave definidas.

1.8.2.5 Efectos

Se espera contar con la documentación necesaria a través de las búsquedas llevadas a cabo. Esto con el fin de comprender en profundidad los algoritmos criptográficos modernos simétricos y asimétricos, incluyendo curvas elípticas y, de esa manera, poseer la noción en cuanto a esfuerzos que se han realizado para introducir la criptografía en los sistemas informáticos modernos.

1.8.2.6 Medida de resultado

Se usan los parámetros definidos en SCImago Journal Rank, con el fin de evaluar la calidad de las fuentes resultantes que se utilizan.

1.8.2.7 Población

La población del presente estudio corresponde a los informáticos en general, de las empresas privadas y entidades públicas en el ámbito global.

1.8.2.8 Aplicación

La presente investigación tiene como finalidad ser una guía para los informáticos en las áreas de ciberseguridad, desarrollo, infraestructura, analistas, computación en la nube, científicos de datos, especialistas en *blockchain* y personas entusiastas sobre el tema.

1.8.2.9 Diseño experimental

Durante el diseño experimental se realiza un análisis y clasificación de los estudios y artículos científicos que se obtienen con base en la calidad de los argumentos y su relevancia para la presente investigación. Con lo mencionado, se respalda la solidez de la información de autores de peso, lo que permite reducir el rango de estudio, con el fin de generar los resultados que se esperan.

1.8.2.10 Identificación de fuentes

A continuación, se especifican las fuentes fiables para sustentar el proyecto.

1.8.2.11 Definición de criterios de selecciones de fuentes

Los criterios para la validación de las fuentes se fundamentan en los parámetros que facilita SCImago Journal Rank con respecto a la estadística de la influencia científica de las revistas académicas de acuerdo con el número de citas en otros medios y periódicos o revistas de importancia e incluso la familia de donde provengan. A partir de lo anterior se desprenden los siguientes parámetros para la evaluación:

H-index: Hace referencia al número de artículos de la revista que han recibido al menos “h” (cantidad) de citas.

Cuartiles: Los grupos temáticos de las revistas se clasifican en 4 cuartiles: Q1, Q2, Q3 y Q4. Las revistas que poseen mayor prestigio se encuentran dentro del área que ocupa el primer cuartil (Q1).

SCJ (SCImago Journal Rank): Expresa la media de citas ponderadas recibidas en el año en cuestión por los documentos publicados en la revista o editorial en los 3 años anteriores.

Citación por documento: Se refiere al número de documentos citados al menos una vez en los 3 años anteriores.

1.8.2.12 Lenguaje de los estudios

Para el estudio se utiliza el idioma español, portugués e inglés con respecto a las búsquedas, de esta forma, se amplía el rango de posibles resultados.

1.8.2.13 Identificación de fuentes

Se describe la selección llevada a cabo correspondiente a las fuentes que se utilizan para la documentación primaria. A la vez, se describe la ejecución de las búsquedas, lo que da como resultado la generación de una lista de fuentes.

1.8.2.14 Métodos identificación de fuentes

El método de selección de las fuentes se fundamenta primordialmente en el respaldo que posea la fuente como tal en el área informática y criptográfica en cuanto a la publicación de estudios y documentos investigativos. Además, se valora la viabilidad del acceso a los sitios con respecto a las búsquedas.

1.8.2.15 Cadenas de búsqueda

Para las búsquedas se utilizarán las siguientes cadenas: “criptografía simétrica y asimétrica”, “técnicas criptográficas”, “algoritmos de hash”, “criptografía moderna”, “criptografía de curvas elípticas”, “criptografía y seguridad”, “criptografía y medios digitales”, “criptografía en la comunicación” entre otras.

1.8.2.16 Lista de fuentes

Debido a la inmensa cantidad de documentación y artículos académicos actuales que se basan en el tema de investigación, se consideran principalmente (aunque no se limita) las siguientes fuentes:

- NIST
- OWASP
- PCI DSS
- CCN-CERT
- FIPS
- IEEE
- ISO

- IETF

Capítulo 2. Marco teórico o conceptual

Se genera la nube de conceptos con el objetivo de identificar los términos más sobresalientes que se obtienen a través de las búsquedas definidas en las diversas fuentes como parte del estado de la cuestión.

Figura 2: Nube de palabras

Elaborado en https://www.nubedepalabras.es/

2.1 Criptografía

Desde sus inicios, la humanidad se ha comunicado a través de distintos medios, los cuales han evolucionado al mismo tiempo que evoluciona el conocimiento y la tecnología. No obstante, la información debía entregarla y comprenderla únicamente por el destinatario correspondiente, por lo tanto, se empezaron a utilizar diferentes medidas para ocultar la información inteligible en información sin sentido, de manera que solo aquel que tuviera la combinación correcta (clave) puede tornar la información a su estado original y comprenderla como el emisor lo deseaba.

En la actualidad, se realiza el mismo procedimiento con técnicas mucho más sofisticadas que involucran muchas áreas de la ciencia como las Matemáticas, la Criptografía, la Criptoanalítica y la Informática. En cuanto a la criptografía, PCI DSS (2015) brinda una descripción por medio de su glosario:

Disciplina de las matemáticas y la informática que se ocupa de la seguridad de la información, en particular el cifrado y la autenticación. En las aplicaciones y la

seguridad de la red es una herramienta para el control de acceso, la confidencialidad y la integridad de la información (s. p.).

Conforme a la complejidad y robustez que la criptografía ha obtenido hasta la actualidad, también crecen las opciones para las organizaciones y desarrolladores. Una selección inapropiada en la criptografía por utilizar puede resultar en la ilusión en cuanto a la seguridad, pero representar poca e incluso nula seguridad en donde se implemente. Debido a esto, la presente investigación se enfoca en la criptografía simétrica y asimétrica incluyendo curvas elípticas, las cuales se encuentran entre los primeros lugares en cuanto a protección (aprobados) se refiere.

Para transformar la información en texto o datos encriptados/cifrados se necesita de un algoritmo criptográfico o también conocido como algoritmo de encriptación o algoritmo de cifrado. PCI DSS (2015) lo define como: “Secuencia de instrucciones matemáticas que se utiliza para transformar un texto o datos sin cifrar en un texto o datos cifrados, y viceversa” (s. p). De aquí en adelante se utilizan los términos *encriptado* y *cifrado*, así como *desencriptado* y *descifrado* de forma indistinta.

2.1.1 Usos de la criptografía

El uso de la criptografía se ha extendido de forma vertiginosa debido a que proporciona una fuerte seguridad en los servicios en donde se implementa, los cuales tienen como objetivo la confidencialidad, autenticación de identidad, autenticación de integridad, autenticación de recursos, autorización y no repudio.

2.1.1.1 Autenticación

Según NIST Special Publication 800-57 Part 1 Revision 5 (2020): “Un proceso que garantiza el origen y la integridad de la información en sesiones de comunicación, mensajes, documentos o datos almacenados o que garantiza la identidad de una entidad que interactúa con un sistema” (s. p.).

Los tipos de autenticación son: autenticación de identidad, autenticación de integridad y autenticación de fuente.

2.1.1.2 Autorización

De acuerdo con PCI DSS (2015): “En el contexto del control de acceso, la autorización es la concesión de acceso u otros derechos a un usuario, programa o proceso. La autorización define lo que un individuo o programa puede hacer después de una autenticación exitosa” (s. p).

Antes de otorgar la autorización a un individuo o proceso se debe validar su autenticidad. Es posible otorgar autorización a partir de un rol, el cual comparten muchos individuos y, por lo tanto, los privilegios se asocian al rol.

2.1.1.3 No repudio

Según CCN-CERT (2022): “Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron” (s. p.). El no repudio tiene como objetivo verificar las acciones realizadas, tanto por quien la realiza como quien la recibe. De esta manera, aunque exista autenticación y autorización, las acciones se deben registrar, de tal forma que se pueda validar la autenticidad de la información.

2.1.2 Algoritmos criptográficos aprobados

Conforme a la actual publicación especial de NIST (NIST Special Publication 800-57 Part 1 Revision 5) publicada en el año 2020, se especifican las recomendaciones para la gestión de llaves criptográficas. Se menciona que existen tres tipos de algoritmos criptográficos aprobados, los cuales se clasifican en algoritmos de llave simétrica, algoritmos de llave asimétrica y funciones *hash*. Lo anterior se basa principalmente en dos factores, los cuales se evalúan en el momento de validar la seguridad que proporcionan y estos son el número de llaves criptográficas y el algoritmo que se utiliza para encriptar/desencriptar el texto o datos.

Estado	Descripción
Aceptable (Acceptable)	El algoritmo está especificado en los documentos del NIST o se encuentra entre los algoritmos acreditados por FIPS y puede emplearse sin restricciones debido a que son los más recomendados para gestionar datos sensibles.
Obsoleto (Deprecated)	El uso del algoritmo y de la longitud de clave se permite, sin embargo, el propio usuario debe aceptar riesgos al utilizarlo.
Desaprobado (Disallowed)	El uso del algoritmo o de la longitud de la clave se encuentra obsoleto y hay restricciones adicionales requeridas para procesos de protección criptográfica de datos. Por lo tanto, se desestima su uso como medida de protección criptográfica.

Uso heredado (Legacy-use)	El algoritmo o la longitud de clave puede usarse para procesar datos protegidos previamente como en el caso de desencriptar datos o verificar una firma digital, pero pueden existir riesgos en este proceso.

Tabla 4: Estados de algoritmos criptográficos
Fuente: NIST Special Publication 800-131 Revision 2

En la tabla anterior se hace referencia en este documento únicamente a los algoritmos con estado “Aceptable” (aprobados).

2.1.3 Llave criptográfica

Hasta este punto se ha podido notar la presencia de lo que se le denomina una llave criptográfica o en las literaturas también se le conoce como clave criptográfica, lo cual es el punto vital de un algoritmo criptográfico. PCI DSS (2015) define llave criptográfica de la siguiente forma: “Valor que determina la salida de un algoritmo de cifrado al transformar el texto plano en texto cifrado. La longitud de la clave suele determinar la dificultad de descifrar el texto cifrado de un mensaje determinado” (s. p).

Cada algoritmo posee uno o un conjunto de llaves con longitudes, lo que permite la fortaleza que brinda este algoritmo, cuanto más longitud posea la llave menos posibilidad de encontrar choques entre los resultados que produce.

2.1.4 Uso de llave

Por lo general, las llaves deben tener un solo propósito, como la encriptación, autenticación de integridad, generación de bits aleatorios, firma digital, entre otros. NIST brinda algunas razones por las que las llaves deben tener un único propósito:

- Si la llave tiene más de un propósito en diferentes procesos criptográficos esto puede debilitar la seguridad proveída por uno o cada proceso involucrado.
- Al limitar el propósito de la llave disminuye el daño que puede causar si esta llave se compromete.
- Algunos usos de llaves se interfieren por su naturaleza como en el caso de que una llave destinada para el transporte de llave y otra para firma digital.

Se debe dejar en claro que cuando se menciona que las llaves deben tener un solo propósito es con respecto a lo que fueron destinadas. Es decir, si una llave, por ejemplo, tiene el propósito de proveer autenticación de integridad en las firmas digitales, esta llave debe realizar ese único proceso y no utilizarla para otros procesos distintos.

2.1.5 Criptoperiodos

NIST (2022) brinda una definición bastante clara correspondientemente a los criptoperiodos: “Un cripto periodo es el periodo de tiempo durante el cual una clave específica está autorizada para su uso por entidades legítimas o las claves de un sistema determinado permanecerán en vigor” (s. p). Un criptoperiodo definido debe delimitar al menos los siguientes seis aspectos:

- La cantidad de información que está disponible para que el criptoanálisis revele la clave.
- La cantidad de exposición si se compromete una sola clave.
- El uso de un algoritmo definido (ejemplo: vida útil estimada).
- El tiempo disponible para los intentos de penetrar los mecanismos de acceso físico, lógico y de procedimiento que protegen una clave de la divulgación no autorizada.
- El periodo en el que la información puede verse comprometida por la divulgación inadvertida de una clave criptográfica a entidades no autorizadas.
- El tiempo disponible para el criptoanálisis computacionalmente intensivo.

2.1.6 Llaves comprometidas

Se puede afirmar que la información protegida por un determinado algoritmo criptográfico se encuentra segura únicamente si este algoritmo permanece fuerte y sus llaves no son comprometidas. Los dueños de las llaves privadas tienen la responsabilidad de mantener estas llaves de forma que ningún tercero tenga acceso a estas y así mantener la confidencialidad de los datos encriptados.

En caso de que exista un compromiso de las llaves produciría de inmediato falencias no solo en la confidencialidad, sino también en temas que se relacionan con la integridad. Es debido a lo anterior que se debe revocar la llave que se utiliza una

vez que se hayan tomado las medidas necesarias para realizar el cambio, ya sea de la llave o del propio algoritmo criptográfico según la gravedad del compromiso, lo que implicaría:

- La divulgación no autorizada de una llave permite que otra entidad no autorizada pueda conocer la llave y, de esta manera, utilizarla para realizar cálculos que necesiten su uso.
- Si una llave se compromete y su integridad es afectada en su información, ya sea que haya sido modificada o que se ha sustituido, esto incluye la supresión o la no disponibilidad de la llave. Por lo tanto, la sustitución o modificación de una llave cuyo propósito es proporcionar integridad pone en tela de juicio la integridad de toda la información protegida por esta clave.
- Un compromiso derivado al uso o aplicación de una llave significa que la llave puede utilizarse para un propósito erróneo o para la aplicación incorrecta, lo que da como resultado el compromiso de la información protegida por esta llave.
- El compromiso relacionado con la llave del propietario o entidad significa que la identidad de la organización no puede asegurarse debido a que no se puede saber quién es la entidad.
- Un compromiso asociado entre una llave con otra información ocasiona que no hay asociación del todo o que esta se hizo con la información equivocada. Esto puede generar que los servicios criptográficos involucrados fallen, que se pierda información o que la seguridad de la información se

2.1.7 Confiabilidad de algoritmos y longitud de llaves

En la actualidad, existe una gama bastante amplia de algoritmos criptográficos que pueden utilizarse para la protección de los datos, así como los múltiples usos que hasta el momento se han puesto en evidencia. Además de elegir un algoritmo que satisfaga una determinada necesidad, también se debe analizar y evaluar la longitud de las llaves y la protección que estas proporcionen para el cometido que se pretenda realizar.

No obstante, lo que hoy se considera seguro es probable que no lo sea dentro de un tiempo. Por este detalle, apoyado con las pautas brindadas por NIST se muestra

el estudio realizado en la publicación NIST Special Publication 800-57 Part 1 Revision 5 para el caso de la fortaleza de las llaves con corte en el año 2030:

<table>
<tr><th colspan="2">Fuerza de la seguridad</th><th>Hasta el 2030</th><th>2031 y Adelante</th></tr>
<tr><td rowspan="2">< 112</td><td>Aplicando protección</td><td colspan="2">Desestimado</td></tr>
<tr><td>Procesando</td><td colspan="2">Uso Legacy</td></tr>
<tr><td rowspan="2">112</td><td>Aplicando protección</td><td rowspan="2">Aceptable</td><td>Desestimado</td></tr>
<tr><td>Procesando</td><td>Uso Legacy</td></tr>
<tr><td>128</td><td rowspan="3">Aplicando protección y procesamiento de la información que ya se encuentra protegida</td><td>Aceptable</td><td>Aceptable</td></tr>
<tr><td>192</td><td>Aceptable</td><td>Aceptable</td></tr>
<tr><td>256</td><td>Aceptable</td><td>Aceptable</td></tr>
</table>

Tabla 5: Fuerza de la seguridad en las llaves

Fuente: NIST Special Publication 800-57 Part 1 Revision 5

De la tabla anterior se desprende que, a través del poder de la computación, lo que se aprecia como seguro puede que no lo sea en unos años. Además, cuanto menor sea la fuerza del algoritmo o de la longitud de la llave esto implicaría que:

- Si se comparte información y la llave ha sido vulnerada desembocaría en la sospecha de la seguridad de esta información que se ha compartido.
- Si la vulneración recae en el algoritmo empleado, pero no se ha compartido información entonces no habría divulgación debido a que esta todavía es confidencial incluso si también la llave ha sido vulnerada, aunque esto no quiera decir que exista seguridad en un momento posterior.

2.1.8 Estados de las llaves criptográficas

Las llaves criptográficas poseen un ciclo de vida definido en el cual pueden realizar transiciones entre sus estados a partir de su generación y su destrucción. NIST define seis estados en los cuales una determinada llave puede estar en un momento específico:

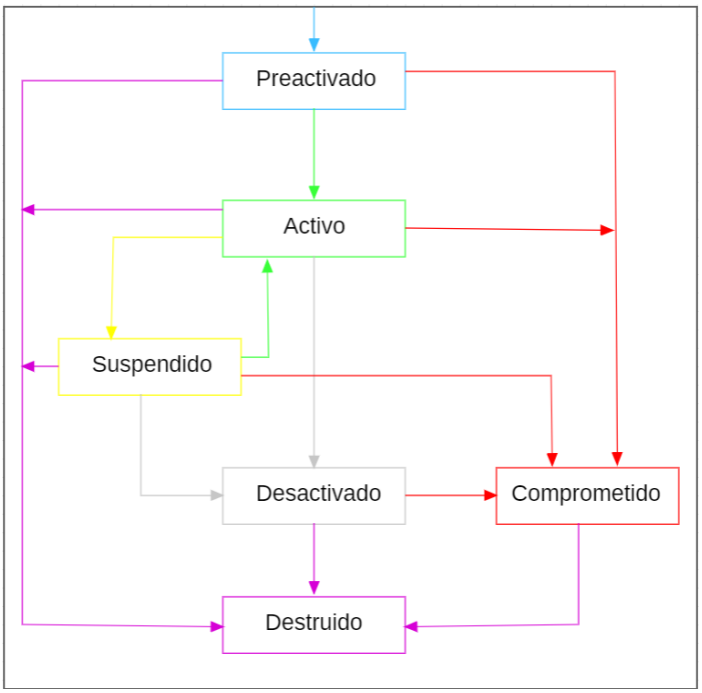

Figura 3: Estados de las llaves criptográficas

Fuente: NIST Special Publication 800-57 Part 1 Revision 5

Con base en la Figura 3 se puede determinar que una llave puede tratarse de forma diferente según el estado del ciclo de vida en la que se encuentre. Por otra parte, los estados de las claves se deben apreciar desde el punto de vista del sistema como tal y no desde la perspectiva de un único módulo criptográfico. A continuación, se explica cada estado de llaves criptográficas:

Estado	Descripción
Preactivado	La llave ha sido generada, pero no está autorizada para utilizarse.
Activo	La llave se encuentra autorizada para usarse en la protección de la información en procesos criptográficos.
Suspendido	La llave se encuentra inhabilitada en espera de ser activada de nuevo o desactivada definidamente.
Desactivado	La llave no puede utilizarse para proteger información en procesos

	criptográficos, sin embargo, en determinados casos puede usarse para procesos *legacy*.
Comprometido	La llave la proporciona y determina por un individuo o entidad no autorizada, por lo tanto, no puede continuar protegiendo la información en procesos criptográficos.
Destruido	La llave se destruye, es decir, deja de existir. No obstante, algunos metadatos de la llave (nombre de la llave, tipo, criptoperiodo, entre otros) pueden permanecer con propósitos de auditoría.

Tabla 6: Descripción de estados de las llaves criptográficas
Fuente: NIST Special Publication 800-57 Part 1 Revision 5

2.1.9 Elección de los algoritmos criptográficos

Cuando se habla de criptografía moderna existen dos componentes básicos, los cuales se encuentran enlazados y, a la vez, definen el resultado por obtener, estos componentes son el algoritmo y la llave. El algoritmo en palabras sencillas se define como la función matemática, en cuanto a la llave es un parámetro que utiliza el algoritmo para realizar el proceso de criptografía (encriptar/desencriptar). Tanto el algoritmo como la llave se utilizan de manera conjunta con el propósito de aplicar protección criptográfica en los datos. La seguridad de la protección en la criptografía se basa en el secreto de la llave que se utiliza y no en el secreto sobre el algoritmo que se emplea, ya que las especificaciones de los algoritmos pueden estar disponibles públicamente.

Las llaves que utilizan los algoritmos pueden establecerse de forma manual, por ejemplo, utilizando un Trusted Courier (mensajería de confianza), la cual puede ser un servicio que se brinda por una determinada empresa o utilizando un método automático. Cuando se utiliza el método automatizado se requiere que exista la autenticación de la fuente, es decir, entre las entidades que participan en la

comunicación, lo cual se lleva a cabo a través de una infraestructura segura como la PKI o *public key infrastructure* (infraestructura de llave pública) cuya definición se deriva a la siguiente: “Un marco establecido para emitir, mantener y revocar certificados de clave pública” (NIST, 2020, s. p).

Además, como se mencionó en los puntos anteriores, las llaves deben utilizarse para un único propósito, ya que si se utiliza la misma llave para diferentes procesos criptográficos aumenta la posibilidad de debilitar la seguridad por uno o ambos procesos.

2.1.9.1 Estándares en los algoritmos criptográficos

Cuando se trata de seguridad y protección en los datos en redes y sistemas informáticos no se debe escatimar la información que proporcionan los estudios e investigaciones realizadas por individuos u organizaciones cuyo objetivo es mantener las mejores prácticas en los diferentes campos de la seguridad informática. En este caso en particular directamente en el campo de la criptografía.

A través de los estudios e investigaciones serias las compañías que se desarrollan en el ámbito de la seguridad informática llegan a consensos en donde se determinan las tecnologías y los pasos del tema determinado. Esto implica la creación de estándares que después pueden utilizar otras personas, empresas u organizaciones debido a los múltiples beneficios que se definen como:

- Prácticas comunes
- Metodología
- Medidas
- Métricas

Las evaluaciones de los estándares las ponen a prueba profesionales en el tema, después las revisa el público en general y, finalmente, las acepta la comunidad de usuarios en general. Los estándares proporcionan beneficios definidos, los cuales se detallan a continuación:

Beneficio	Descripción
Interoperabilidad	Permite a las organizaciones el desarrollo de productos, los cuales poseen la capacidad de comunicarse entre sí debido a que comparten estándares que proporcionan formas estandarizadas de comunicaciones.
Seguridad	Permite establecer niveles de seguridad comunes y definidas.
Calidad	Permite estandarizar y, a la vez, asegurar la calidad de los productos.
Forma común de referencia	Las organizaciones que se encargan de los estándares se toman como referencias para el desarrollo, pruebas y evaluaciones de los productos.
Ahorro de costos	Disminuye el costo en las implementaciones debido a que son el producto de investigaciones de decenas e incluso cientos de profesionales de distintas áreas que brindan sus conocimientos para establecer las mejores medidas por tomar en cuenta.

Tabla 7: Beneficios de los estándares

Fuente: NIST Special Publication 800-175B Revision 1

2.1.9.2 Procesamiento de estándares y publicaciones especiales

La estandarización de las tecnologías y protocolos de comunicaciones, así como métodos y procedimientos para llevar a cabo distintos tipos de comunicaciones entre los sistemas, redes y cualquier cosa en intranet e incluso Internet se maneja a través de estándares. Los cuales se analizan, se implementan, se evalúan y, posteriormente, se brindan a la comunidad a través de publicaciones especiales y estándares realizados por grandes organizaciones cuya misión es establecer lo

correspondiente a temas muy diversos como las matemáticas, informática, robótica, entre otros.

Para el tema relacionado a la criptografía existen organizaciones que definen los estándares para seguir mejorando la seguridad en los entornos digitales. A continuación, se muestran las organizaciones más relevantes en este tema:

Nombre	Descripción
FIPS (Norma Federal para el Procesamiento de Información)	Desarrolla los estándares en el gobierno federal con temas que se relacionan con la protección de información sensible.
NIST (Instituto Nacional de Estándares y Tecnología)	A través de NISTIR (Informe interinstitucional/interno del NIST) desarrollado por NIST de forma interina o en colaboración con otras agencias. Una de las funciones principales de NISTRS es presentarse como investigaciones que apoyan a los trabajos realizados por FIPS y las publicaciones especiales.
ANSI (Instituto Nacional Estadounidense de Estándares)	No desarrolla estándares por sí mismo, sin embargo, facilita los medios para el desarrollo de estándares a través de establecimientos de consensos entre grupos expertos.
IEEE (Instituto de Ingenieros Eléctricos y Electrónicos)	Es una asociación internacional de profesionales dedicados al avance de la innovación y excelencia tecnológica. Su objetivo técnico se centra en el avance en la teoría y práctica en las áreas eléctricas, electrónicas, informática y ciencias de la computación.
IETF (Grupo de Trabajo de Ingeniería de Internet)	Es una comunidad internacional de expertos en diseño de redes, operadores, vendedores, investigadores

	y tecnólogos quienes trabajan construyendo la arquitectura de Internet, sus técnicas y protocolos.
ISO (Organización Internacional de Estandarización)	Es una federación mundial no gubernamental de organismos nacionales de estandarización. Su misión es desarrollar normas internacionales que ayuden a la industria a ser más eficiente y eficaz.

Tabla 8: Organizaciones y estándares

Fuente: NIST Special Publication 800-175B Revision 1

2.2 Funciones hash criptográficas

Las funciones *hash* las usan algunos tipos de algoritmos criptográficos como forma de trasformar los datos. NIST (2020) las define de la siguiente forma: “Una función que mapea una cadena de bits de longitud arbitraria (aunque acotada) a una cadena de bits de longitud fija” (s. p).

2.2.1 Características

Las funciones *hash* para considerarse como aprobadas por NIST deben poseer las siguientes dos características:

- Unidireccional: Es computacionalmente inviable encontrar cualquier entrada a partir de una salida preestablecida.
- Resistente a las colisiones: Es inviable desde el punto de vista matemático e informático encontrar dos entradas distintas que den lugar a la misma salida.

Para explicar los puntos anteriores se presenta la siguiente figura en donde se pueden apreciar las características y funcionalidad de una función *hash*.

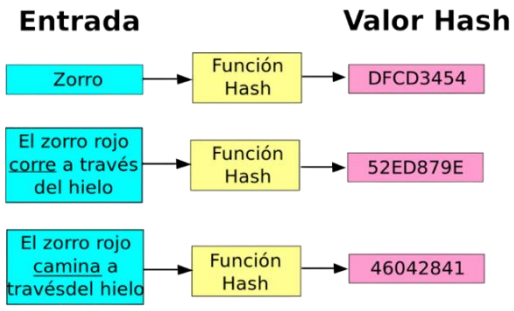

Figura 4: Función hash

Fuente: Kaspersky (2022).

2.2.2 Generación y verificación de los hashes

Las funciones *hash* tienen diversos usos dentro de la computación, los cuales en su forma más simple se basan en los siguientes cuatro pasos:

Generación del *hash*:

1) Se genera un valor *hash* a partir de un valor inicial utilizando una función *hash*.
2) Tanto el valor original como el valor *hash* se almacenan y transmiten.

Verificación del *hash*

3) Se genera un nuevo valor *hash* a partir del valor transmitido (valor original del punto 1) utilizando la misma función *hash*.
4) Se comparan los valores *hash* que se generan en el punto 1 y 3, si ambos son iguales significa que el valor original (punto 1) no ha sido alterado durante el almacenamiento o la transmisión.

2.2.3 Usos

Como se mencionó, las funciones *hash* tienen muchos usos en la actualidad, aunque es muy común utilizarlas a través de algoritmos de alto nivel como los que se mencionan a continuación:

- Algoritmos de código de autenticación de mensajes con clave *hash*.
- Algoritmos de firma digital.
- Funciones de derivación de claves.
- Generadores de bits aleatorios.

2.2.4 Funciones hash aprobadas

Se presentan las funciones *hash* aprobadas en la actualidad, para el uso de seguro de encriptación de datos que se basa en las siguientes publicaciones de NIST FIPS PUB 180-4, FIPS PUB 202 y NIST Special Publication 800-185:

- Familia SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256)
- Familia SHA-3 (SHA3-224, SHA3-256, SHA3-384 y SHA3-512)
- SHAKE128, SHAKE256, cSHAKE, KMAC, TupleHash y ParallelHash (funciones hash de longitud variable)

2.3 Criptografía simétrica

La criptografía simétrica pertenece al grupo de criptografía moderna, la cual, con base en la definición de CCN-CERT (2022) a través de su glosario permite definirlo de la siguiente manera: “Algoritmo para realizar el cifrado o el algoritmo correspondiente para realizar el descifrado en el cual se requiere la misma clave para el cifrado y el descifrado” (s. p.).

Con base en la definición anterior, la criptografía simétrica (también conocida como criptografía de llave simétrica o criptografía de llave secreta) tiene la capacidad de transformar (encriptar) los datos utilizando una determinada llave criptográfica. De esta forma, es fundamentalmente difícil volver a trasformar estos datos a su texto original sin utilizar el mismo algoritmo y llave secreta que se utiliza en el proceso de encriptación. Por lo tanto, cuando se hace referencia a que una llave es simétrica se debe a que la misma llave se utiliza tanto en el proceso de encriptación como en el proceso de desencriptación.

Debido a que la llave en este tipo de criptografía es la misma, tanto para encriptar como para desencriptar, se tiene por sentado que esta llave es conocida por más de un individuo o entidad y, de esa manera, se produce la comunicación. No obstante, aunque la llave es compartida por entidades autorizadas, el proceso de generación de la llave debe hacerse a través de un proceso aleatorio y no debe divulgarse a entidades no autorizadas a acceder los datos protegidos por el algoritmo y la llave.

Cuando se hace referencia al texto original se denomina *plain text* (texto plano) mientras que al texto encriptado se denomina *cipher text* (texto cifrado).

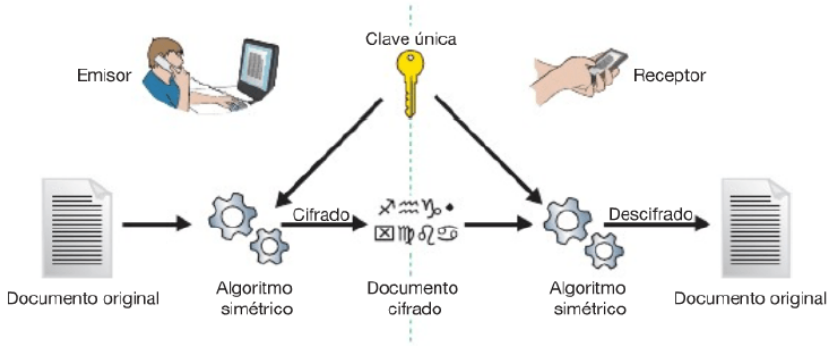

Figura 5: Criptografía de llave simétrica

Fuente: Salmón Corporation (2022).

En la actualidad, existen varias clases de algoritmos criptográficos de llave simétrica que son aprobados por NIST y FIPS:

- Con base en algoritmo de cifrado por bloques
- Con base en el uso de funciones hash.

2.3.1 Usos

La criptografía simétrica se utiliza para diversas actividades cuyo propósito es la de velar por la protección de los datos digitales. En este ámbito se mencionan algunos usos en donde su utilización es muy amplia:

- Encriptación para garantizar la confidencialidad de los datos.
- Autenticación para garantizar la integridad de los datos y su fuente.
- Derivación de claves.
- Envoltura de la clave.
- Generación de *bits* aleatorios.

Un detalle que se debe tener presente con los algoritmos simétricos es que debido a su naturaleza basada en una única llave para habilitar la encriptación/desencriptación de los datos de extremo a extremo, se recomienda que esta llave se genere con el propósito de utilizarse en un único proceso de comunicación. Lo anterior ya que si se utiliza en varios procesos distintos (técnicamente posible utilizando el mismo algoritmo criptográfico), además, se usa múltiples algoritmos criptográficos, puede llegarse el caso en que exista debilidad en

la seguridad de la llave debido a que algunos algoritmos utilizan la misma función *hash* para retornar el valor de la llave resultante. Esto claramente se puede deducir en colisiones entre los valores resultantes.

2.3.2 Tipos de cifrados para criptografía simétrica

Para realizar el cifrado de los datos, la criptografía simétrica usa técnicas como el cifrado por bloques o con base en *hash*, los cuales se detallan en breve.

2.3.2.1 Algoritmos de cifrado por bloques

Para estar sincronizados con el término cifrado por bloques, NIST (s. f.) brinda la siguiente definición:

Un algoritmo criptográfico de clave simétrica que transforma un bloque de información a la vez utilizando una clave criptográfica. Para un algoritmo de cifrado por bloques de bloque, la longitud del bloque de entrada es la misma que la del bloque de salida (s. p.).

A continuación, se muestra el cifrado por bloques usando el modo de operación ECB (libro de códigos electrónico) cuya funcionalidad permite mostrar de forma muy básica el proceso de cifrado (Véase la sección “modos de operación”).

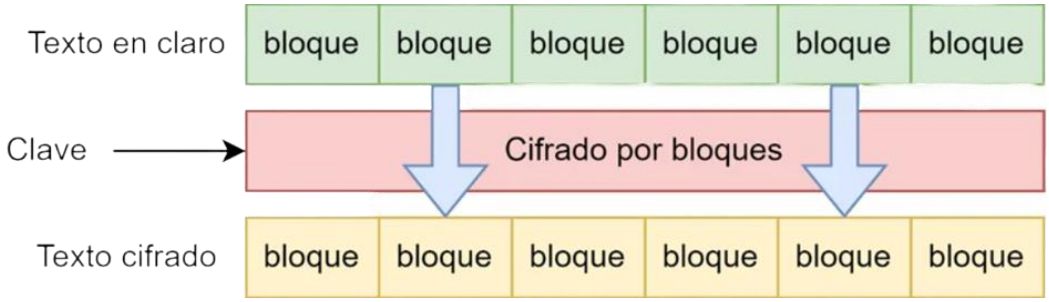

Figura 6: Cifrado por bloques

Fuente: IberAsyn.es (2022).

A continuación, se muestra un listado con los algoritmos criptográficos simétricos NIST en su publicación especial 800-175B revisión 1:

Algoritmos con base en cifrado por bloques	
Algoritmo	**Descripción**
TDEA (Algoritmo de encriptación de datos triple)	Conocido también como Triple DES (encriptación estándar de datos). Encripta bloques de longitudes fijas de 64 bits utilizando un conjunto de tres llaves, las cuales se utilizan una detrás de la otra para obtener, finalmente, un resultado. Posee dos variantes: 2TDEA (la primera y tercera llave son idénticas) y 3TDEA (las tres llaves son diferentes). 2TDEA se encuentra con estado desaprobado mientras 3TDEA se encuentra Obsoleta y se desaprobará a finales del año 2023.
AES (Estándar de Encriptación Avanzada)	Desarrollado como sucesor, tanto de DES como de TDEA. Es el algoritmo de cifrado por bloque preferido para los nuevos productos. Utiliza bloques de 128 bits y llaves de 128, 192 y 256 bits.

Tabla 9: Algoritmos con base en cifrado por bloques

Fuente: NIST Special Publication 800-175B Revision 1

2.3.2.2 Modos de operación

Con los algoritmos de cifrado por bloques de clave simétrica, al utilizar una determinada llave, el mismo bloque de entrada produce siempre el mismo bloque de salida. Existe la posibilidad de que, si los múltiples bloques de un determinado mensaje se cifran por separado, un adversario pueda reemplazar estos bloques de forma individual y, en el peor de los casos, sin detectarse. Además, patrones repetidos en el texto plano serían evidentes en el texto cifrado.

Debido a lo anterior, para contrarrestar este tipo de problemas se han especificado modos de funcionamiento para utilizar un algoritmo de cifrado por bloques. A continuación, se muestran los modos de cifrado para los algoritmos simétricos aprobados por NIST:

Abreviación del modo	Nombre del modo
ECB	Electronic Code Book (libro de códigos electrónico)
CBC	Cipher Block Chaining (encadenamiento de bloques de cifrado)
CFB	Cipher Feedback (comentarios del cifrador)
OFB	Output Feedback (comentarios de la salida)
CTR	Counter (contador)
TCBC	Triple DES Cipher Block Chaining (encadenamiento de bloques de cifrado triple DES)
CBCM	CBC with OFB Masking (CBC con enmascaramiento OFB)
INNER-CBC	INNER-CBC (CBC interno)

Tabla 10: Modos de cifrado de algoritmos de llaves simétricas

Fuente: NIST Special Publication 800-175B Revision 1

2.3.2.3 Algoritmos de cifrado con base en función hash

Aquellos algoritmos de llave simétrica con base en funciones *hash* tienen como fin generar un código de autenticación de mensaje (MAC). NIST (2020) define código de autenticación de mensaje como: **"**Una suma de comprobación criptográfica de datos que utiliza una función de seguridad aprobada y una clave simétrica para detectar tanto las modificaciones accidentales e intencionadas de los datos**"** (s. p). A continuación, se listan las funciones *hash* aprobadas:

Abreviación de la función	Nombre de la función
CSHAKE	Customable version SHAKE (versión personalizable de SHAKE)
KMAC	KECCAK Message Authentication Code (código de autenticación de mensaje KECCAK)
TupleHash	Tuple Hash (tuplas de *hash*)
ParallelHash	Parallel Hash (*hash* paralelo)

Tabla 11: Algoritmos de cifrado con base en funciones hash

Fuente: NIST Special Publication 800-175B Revision 1

2.4 Criptografía asimétrica

La criptografía asimétrica (también conocida como criptografía de llave pública) al igual que la criptografía simétrica pertenece al grupo de criptografía moderna. La corporación Kaspersky (2022) a través de su glosario permite definirlo de la siguiente manera:

En este tipo de cifrado, se utilizan dos claves diferentes (pública y privada) que están vinculadas entre sí matemáticamente. Las claves son básicamente números extensos vinculados entre sí, pero no son idénticos; de ahí el término asimétrico. El propietario mantiene en secreto la clave privada, mientras que la clave pública se comparte entre los receptores autorizados o queda disponible al público general (s. p).

A diferencia de las llaves simétricas en donde para cada establecimiento de comunicación entre entidades se necesita un par de llaves, es decir, si hubiese 100 entidades deseando establecer una comunicación segura con una entidad determinada, se necesitarían 100 pares de llaves debido a que, para cada comunicación con una entidad, la organización tiene que generar una clave diferente. El mismo caso, pero con llaves asimétricas es muy distinto, ya que se necesitaría un par de llaves, una privada que es la que salvaguarda la organización y la pública puede compartirse por las 100 entidades.

En este tipo de criptografía asimétrica, ambas llaves pueden utilizarse para cifrar o descifrar los datos. Sin embargo, este proceso solo puede hacerse entre el par de llaves correspondientes, es decir, la llave privada y la llave pública

correspondiente, no obstante, el proceso depende del tipo de flujo que tenga la comunicación:

1) Cuando la llave privada es la que cifra, únicamente aquellas personas u organizaciones que posean la llave pública pueden descifrar los datos.
2) Cuando la llave pública es la que cifra, únicamente quien posea la llave privada puede descifrar los datos.

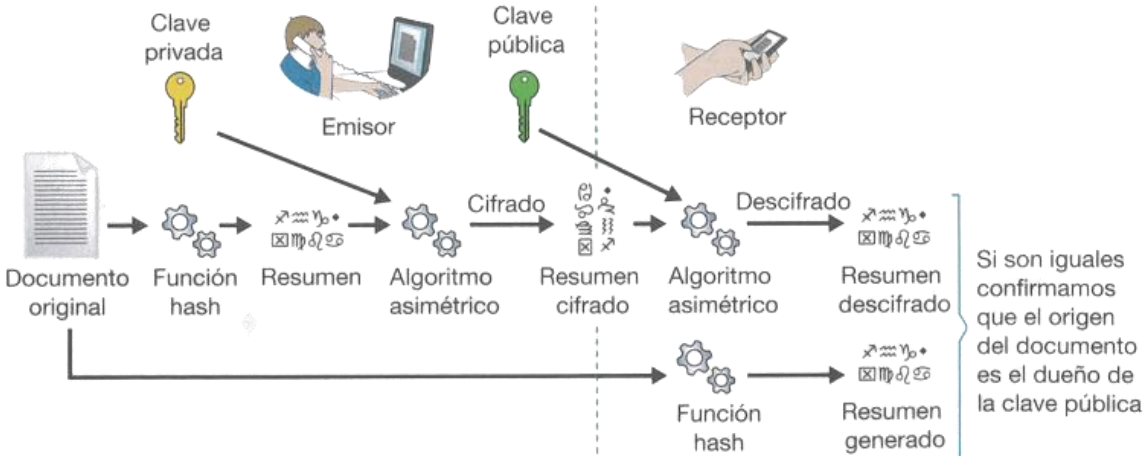

Figura 7: Criptografía de llave asimétrica

Fuente: Salmón Corporation (2022).

2.4.1 Usos

- Proporcionar formas de servicios de identidad, integridad y autenticación de fuentes en forma de firmas digitales.
- Establecer el material de clave criptográfica utilizando el acuerdo de clave y el algoritmo de transporte de clave.

Al igual que las llaves de la criptografía simétrica, el par de llaves de la criptografía asimétrica deben generarse para un único propósito, ya que, de esta manera, se evita la debilitación de la eficacia de la seguridad brindada por los algoritmos a través de múltiples propósitos. Para simplificar el uso y tipo de pares de llaves asimétricas se hace una separación entre aquellas con algoritmos para firma digital y los de esquemas de establecimiento de llaves.

Algoritmos de firma digital	
Nombre	Descripción
DSA "Digital Signature Algorithm" (algoritmo de firma digital)	Se utiliza para generar y verificar firmas digitales usando campos finitos. FIPS 186 determina los métodos para generar los parámetros, pareja de llaves y longitudes de llaves para validar la seguridad que se brinda en los procesos de firma digital.
ECDSA "Elliptic Curve Digital Signature Algorithm" (algoritmo de firma digital de curva elíptica)	Tanto el algoritmo de verificación y de firma básica son iguales a los de DSA con la diferencia que en lugar de utilizar la matemática de campos finitos, ECDSA utiliza curvas elípticas. Además, posee longitudes de llaves mucho más cortas y requiere menos espacio de almacenamiento y ancho de banda para la transmisión. La ejecución del algoritmo es más rápida al utilizar menos poder de computación para calcular la llave.
EdDSA "Edwards-curve Digital Signature Algorithm" (algoritmo de firma digital de la curva de Edwards)	Las firmas de EdDSA son deterministas, es decir, el valor único de la llave se computa usando la llave privada y el propio mensaje por firmarse, por lo tanto, no se requiere un generador aleatorio de bits para su creación.
RSA (Rivest, Shamir y Adleman)	FIPS 186 determina las restricciones correspondientes para el uso de RSA en donde se incluyen la generación del par de llaves, métodos y longitud de llaves.

Tabla 12: Algoritmos de firma digital

Fuente: NIST Special Publication 800-175B Revision 1

Esquemas de establecimiento de claves	
Nombre	Descripción
Diffie−Hellman (DH) and MQV (Diffie−Hellman y MQV)	Puede utilizar tanto matemática de campos finitos como matemáticas de curvas elípticas. Para campos finitos, se puede seleccionar un grupo de dominio de parámetros del listado de SP 800-56 A o generarlos al igual que el dominio de parámetros par DSA. Para curvas elípticas, los métodos que se utilizan para la generación de llaves se obtienen a partir del listado que brinda FIPS 186.
RSA (Rivest, Shamir y Adleman)	Debido a que RSA puede utilizarse tanto para establecimiento y generación de llaves para firma digital, es recomendable no utilizar la misma llave para ambos propósitos.

Tabla 13: Esquemas de establecimiento de claves

Fuente: NIST Special Publication 800-175B Revision 1

2.5 Criptografía de curvas elípticas

La criptografía de curvas elípticas o simplemente ECC (Elliptic Curve Cryptography) la define PCI DSS (2022) a través de su glosario como: “Enfoque de la criptografía de clave pública basada en curvas elípticas sobre campos finitos” (s. p).

El enfoque del presente estudio se basa en el análisis y aplicación de las criptografías que se relacionan con el tema de investigación y, por ende, se ha omitido la parte matemática en su funcionamiento. No obstante, para la criptografía de curvas

elípticas se hace una leve excepción, ya que para tener claro cómo funcionan se debe abordar la matemática, aunque no se profundiza debido a que el objetivo es explicar su funcionamiento.

Este tipo de criptografía permite la obtención de llaves privadas y públicas, lo que posibilita compartir y resguardar estas llaves de manera muy segura, tanto así que se considera tan segura como la criptografía de llave pública más seguras en la actualidad, además de que agrega eficiencia, velocidad y escalabilidad.

2.5.1 Qué es la criptografía de curva elíptica

La criptografía de curvas elípticas tiene un enfoque sobre la creación de sistemas cifrados asimétricos o también conocido como sistema de llave pública/privada. No obstante, se diferencia en que utiliza estructuras algebraicas de curvas elípticas sobre campos finitos, con el fin de garantizar la seguridad y fiabilidad sobre los procesos criptográficos que realiza. Lo anterior sumado a que permite que las llaves sean de menor tamaño que las habituales en otros sistemas criptográficos sin afectar en ningún modo la seguridad que proporciona.

Las funciones matemáticas en las que se basa la criptografía de curvas elípticas son simples de calcular de forma unidireccional, no así de forma inversa, ya que es extremadamente difícil revertir y obtener el valor inicial que se utiliza. Es decir, crear llaves es sencillo, pero romper su seguridad es prácticamente imposible debido a que es inviable calcular el logaritmo discreto de un determinado elemento de una curva elíptica aleatoria con respecto a un punto base conocido de forma pública.

Es relevante mencionar que la criptografía de curvas elípticas puede combinarse con los esquemas de cifrado simétrico, lo que da como resultado una mayor protección.

2.5.2 Qué son las curvas elípticas

Una curva elíptica es aquella que se forma cuando se aplica la función general de curvas elípticas en un plano cartesiano y se representa con la siguiente denotación: “$y^2 = x^3 + ax + b$”

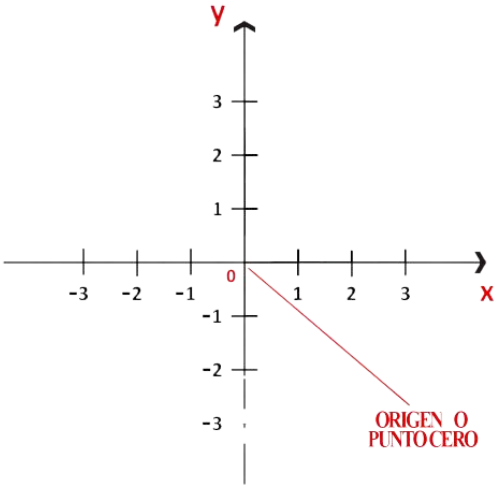

Figura 8: Plano cartesiano

Fuente: www.significados.com

A partir del plano cartesiano, se pueden combinar los elementos de la ordenada (eje Y) con los elementos de la abscisa (eje X), lo que da como resultado, lo que se le denomina coordenadas del plano cartesiano.

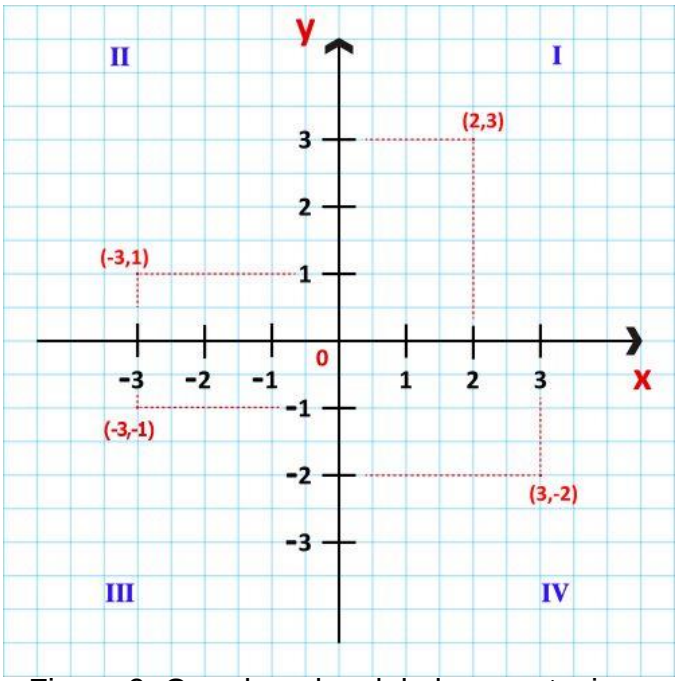

Figura 9: Coordenadas del plano cartesiano

Fuente: www.significados.com

Con base en la fórmula para las curvas elípticas, dentro de un plano cartesiano es posible observar una figura que se dibuja como la siguiente:

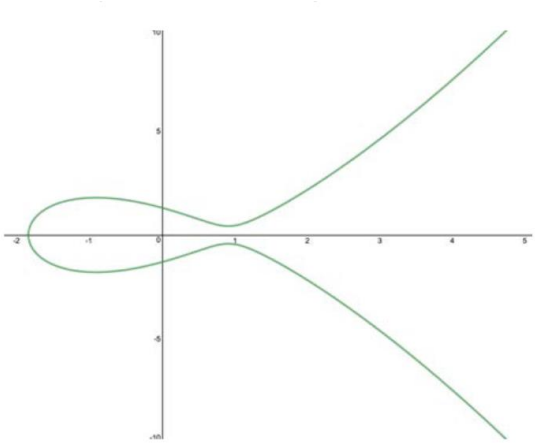

Figura 10: Curva elíptica general en plano cartesiano

Fuente: Applications of Elliptic Curve Cryptography (2017).

La forma de la curva elíptica se define por los valores *a* y *b* de la fórmula que se muestra previamente ($y^2 = x^3 + ax + b$). A continuación, se muestra la forma de la curva cuando se cambian estos valores a través de la herramienta Geogebra:

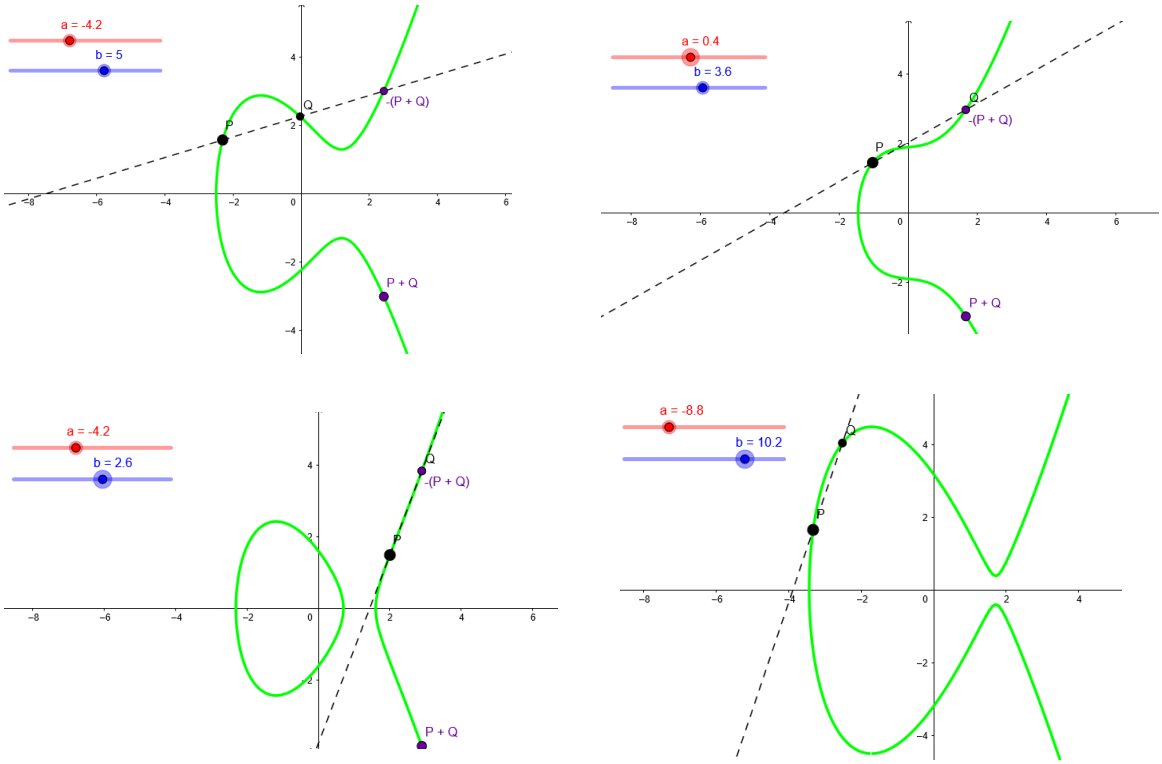

Figura 11: Visualizaciones de la curva elíptica

Fuente: GeoGebra (2022).

2.5.3 Características de las curvas elípticas

Las curvas elípticas deben cumplir con ciertas características para poderse considerar como una curva elíptica válida:

- La curva elíptica es simétrica con relación al eje X.
- La coordenada (0,0) se denomina origen o punto 0.
- La curva no debe intersecarse a sí misma.
- No debe existir la singularidad, es decir, no debe existir ningún punto de la curva en donde dos derivadas parciales sean igual a cero y se expresa con la función: $4a^3+27b^2 \neq 0$.

2.5.4 Curvas elípticas sobre cuerpos finitos

Las curvas elípticas pueden definirse sobre cualquier conjunto de números contenidos en R o números reales (ejemplos: 2,5, 4/3, PI, etc.). Sin embargo, trabajar con estos tipos de números resulta problemático, tanto por la velocidad de cálculo reducida como por la imprecisión que implica realizar operaciones sobre este tipo de números, computacionalmente hablando. Por lo tanto, se definió el conjunto Z o números enteros como el conjunto para construir algoritmos criptográficos de curvas elípticas, ya que limita el campo sobre cuerpos finitos.

$$\mathbb{Z} = \{-\infty, \dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots, \infty\}$$

Figura 12: Conjunto de números enteros

Fuente: GeoGebra (2022).

2.5.5 Selección de longitud de la llave

Se debe tener presente que los principales parámetros de la criptografía de curva elíptica son la curva elíptica denominada como E y un punto designado G en E denominado punto base. El punto base tiene un orden N que a la vez es un número primo grande. El número de puntos en la curva es H·N para algún número entero H (el cofactor) que, a la vez, no es divisible por N. Es deseable que el cofactor sea lo más pequeño posible debido a factores de eficiencia.

2.5.6 Selección de los campos subyacentes

Para cada longitud de llave existen dos tipos de campo, los cuales se listan a continuación:

- Campo primo: Teniendo GF(p) que contiene un número primo *p* de elementos. Los elementos de este campo son los enteros módulo *p* y la aritmética del campo se implementa en términos de la aritmética de los enteros módulo *p*.
- Campo binario: Teniendo GF(2^m) que contiene 2^m elementos para algún *m* (denominado el grado del campo). Los elementos de este campo son las cadenas de *bits* de longitud *m* y la aritmética del campo se implementa en términos de operaciones sobre los *bits.*

Longitud de bits de "n"	Campo primo	Campo binario
224-255	Len(p) = 224	M = 233
256-383	Len(p) = 256	M = 283
384-511	Len(p) = 384	M = 409
≥ 512	Len(p) = 521	M = 571

Tabla 14: Longitud de bits de los campos subyacentes de las curvas recomendadas.

Fuente: Draft NIST Special Publication 800-186 (2019).

2.5.7 Curvas sobre campos primos

Curvas Weierstrass	Curvas Montgomery	Curvas Edwards25519
P-224	Curve25519	Edwards448
P-256	Curve448	E448
P-384		
P-521		
W-25519		
W-448		

Tabla 15: Curvas sobre campos primos

Fuente: Draft NIST Special Publication 800-186 (2019).

2.5.8 Curvas sobre campos binarios

Curvas Koblitz	Curvas Pseudorandom
K-233	B-233
K-283	B-283
K-409	B-409
K-571	B-571

Tabla 16: Curvas sobre campos binarios

Fuente: Draft NIST Special Publication 800-186 (2019).

2.5.9 Curvas elípticas en la criptografía

Debido a que la criptografía de curvas elípticas se basa en la criptografía de llave pública se necesita una llave privada y otra pública para crear una comunicación segura entre las partes que contengan estas llaves. Para entender mejor el uso de las curvas elípticas en la criptografía, a continuación, se describe una comunicación entre dos personas denominadas como Alice y Bob que utilizan la misma curva elíptica para generar los cálculos.

Antes que nada, se debe describir la multiplicación de puntos de una curva elíptica. Si se supone que P es cualquiera de la curva elíptica que se utiliza, entonces la multiplicación de P es sumar repetidamente P una cantidad finita de veces, lo que da lugar a una operación como la siguiente:

$$K * P = P + P + P + \ldots + k \text{ veces.}$$

Siendo P el punto de la curva elíptica y *k* las veces que se suma el punto P.

Teniendo claro el punto anterior, se procede con la suposición de que *n*B es la llave privada de Bob (un punto cualquiera seleccionado entre los puntos que componen la curva elíptica) y G es un generador de números aleatorios. Por lo tanto, para obtener la llave pública de Bob se debe realizar la siguiente multiplicación:

$P_b = nB * G$

Siendo P_b la llave pública.

Ahora Alice desea enviar un mensaje denominado P_m a Bob, para esto, utiliza la llave pública de Bob para encriptar este mensaje, el cual se obtiene de la siguiente manera.

$$P_c = \{k * G, P_m + k * P_b\}$$

En donde *k* hace referencia a un número entero aleatorio. El hecho de que *k* sea aleatorio asegura que incluso para el mismo mensaje el texto generado sea totalmente diferente cada vez.

Al suponer que Bob desea desencriptar el mensaje enviado por Alice, lo primero que hace Bob es sustraer la coordenada definida por "*k* * G" para posteriormente multiplicarla por *n*B a partir de "$P_m + k * P_b$". Esto da como resultado el mensaje original a través de la siguiente operación:

$P_m = \{P_m + (k * P_b) – (n\text{B} * k * \text{G})\}$

En donde P_m es el mensaje enviado por Alice.

De esta manera, se puede observar el mecanismo que utilizan las curvas elípticas en la criptografía para cifrar y descifrar los datos de una manera simplificada.

Capítulo 3. Marco metodológico

3.1 Tipo de investigación

La presente investigación se clasifica como evaluativa debido a que tiene como objetivo proponer un modelo para la selección de algoritmos criptográficos modernos simétricos y asimétricos incluyendo curvas elípticas, aprobados en entornos informáticos. Por lo tanto, se reúne información de estándares y publicaciones para emitir posteriormente un criterio mediante una propuesta.

3.2 Alcance investigativo

El alcance investigativo es descriptivo y se basa en la definición que brinda Vargas (2004): "Tipo de estudio que busca especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a análisis" (s. p.).

En el caso de la presente investigación se considera el estudio y análisis del entorno de la criptografía simétrica y asimétrica incluyendo curvas elípticas, sus características, estados actuales, seguridad brindada, entre otros puntos.

3.3 Enfoque

El enfoque dado a esta investigación es mixto debido a que, por una parte, se utiliza el enfoque cualitativo, ya que se busca evaluar la información resultante a través de la investigación y, a la vez, tomando como referencia los estudios realizados por organizaciones y fuentes reconocidas en donde se pueda comprobar la calidad y credibilidad de los criterios que se utilizan. Por otra parte, se usa el enfoque

cuantitativo, ya que se realiza una medición de eficacia de los algoritmos de forma programada y, posteriormente, se muestran los resultados, de manera que se puedan apreciar las ventajas e impacto en su selección y sus posibles aplicaciones.

3.4 Diseño

El diseño de la investigación es evaluativo, ya que el objetivo principal es el establecimiento de una mejora en el ámbito de la seguridad de la información digital en las organizaciones cuya innovación reside en la propuesta de selección y simplificación de datos para las posibles implementaciones de criptografía simétrica y asimétrica incluyendo curvas elípticas. La investigación implica los siguientes pasos:

- Evaluación de las publicaciones de NIST y FIPS y se filtran los puntos destacados para la investigación.
- Revisión de estándares internacionales establecidos por NIST, FIPS, ISO y PCI con el objetivo de extraer los controles requeridos, lo que da como resultado la generación de una propuesta entre los estándares internacionales.
- Realización de una encuesta difundida por redes sociales con el objetivo de identificar y medir el conocimiento y falencias en cuanto a la selección y uso de la criptografía en las organizaciones.
- Se eligen los algoritmos criptográficos que cumplan con los filtros impuestos en la investigación.
- Explicación de los algoritmos elegidos para justificar y esclarecer su elección.
- Diseño de la propuesta con los algoritmos criptográficos elegidos.
- Análisis final y conclusiones de la investigación.

3.5 Población y muestreo

La presente investigación por su enfoque y estudio no es aplicable a un grupo en particular, el cual pueda ser medible. Esto se debe a que el grupo de estudio son todos aquellos profesionales y entusiastas quienes deseen introducirse en la criptografía e implementar las mejores prácticas con base en estándares internacionales en cuanto a la selección de los algoritmos seleccionados y usar los servicios que se brindan.

3.6 Instrumentos de recolección de datos

El instrumento de recolección de datos que se utiliza para el presente estudio es el cuestionario generado a través de los formularios de Google, conformado por

siete preguntas específicas sobre la criptografía simétrica, asimétrica y de curvas elípticas. Además, el idioma español se utilizó para la redacción de la encuesta que, a la vez, se publicó en redes sociales y redes profesionales.

3.7 Técnicas de análisis de información

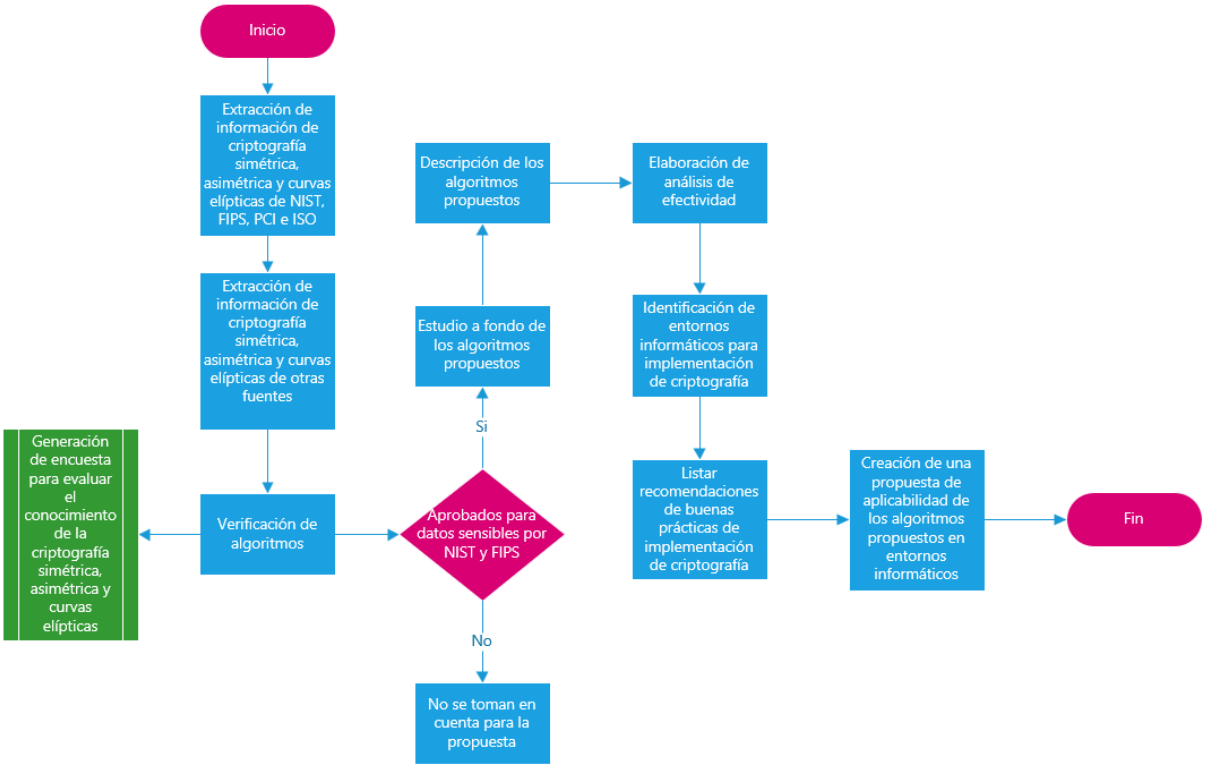

Figura 13: Diagrama de flujo de análisis de la información

Capítulo 4. Análisis del diagnóstico

En este capítulo se detalla el resultado obtenido con base en los objetivos de la presente investigación, la cual se ha canalizado a través de la encuesta y el análisis documental.

4.1 Encuesta

El objetivo de la encuesta se basa en la identificación del conocimiento general de las personas (en su mayoría que se relacionan con la tecnología) en cuanto a la criptografía simétrica y asimétrica incluyendo curvas elípticas aplicadas en su vida laboral o cotidiana, a través de buenas prácticas en la implementación de estas con base en las distintas ventajas que cada una proporciona para brindar seguridad a los datos digitales. La encuesta como tal tiene un formato breve y sencillo con preguntas cerradas y, a la vez, utiliza vocabulario fácil de asimilar con el objetivo de atraer a la

mayor cantidad de audiencia en el menor tiempo siempre manteniendo el anonimato para conformidad de las personas encuestadas.

4.2 Distribución

La encuesta se realizó a través de la herramienta de formularios de Google y se distribuyó por redes sociales como LinkedIn y empresas informáticas nacionales que por motivos de solicitud se mantienen en anonimato.

4.3 Encabezado

Se detalla de forma introductoria a la encuesta con el objetivo de aclarar el tema y la intención relacionada con la criptografía.

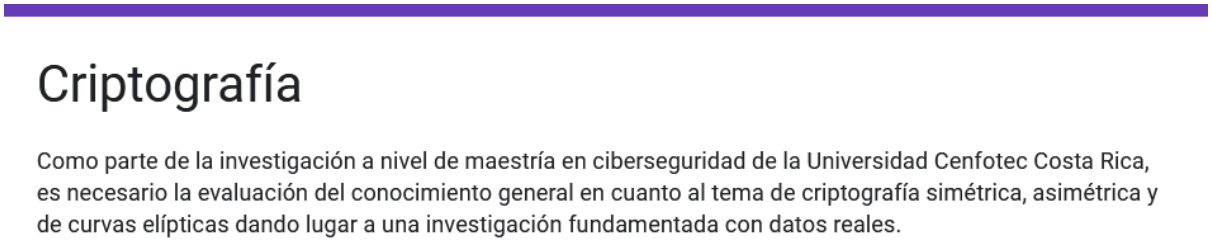

Figura 14: Encabezado de la encuesta

4.4 Preguntas

La encuesta cuenta con siete preguntas en su totalidad, las cuales se exponen a continuación.

4.4.1 Pregunta n.º 1

¿En cuál área trabaja? Con nueve opciones: Desarrollo de *software*, QA, ciberseguridad, analista de sistemas informáticos, especialista en computación en la nube, especialista en inteligencia artificial, científico de datos, otra área informática, otra área no informática. El objetivo de esta pregunta es localizar las áreas en las cuales las personas laboran y la frecuencia con la que utilizan la criptografía como medio para proteger los datos que manipulan.

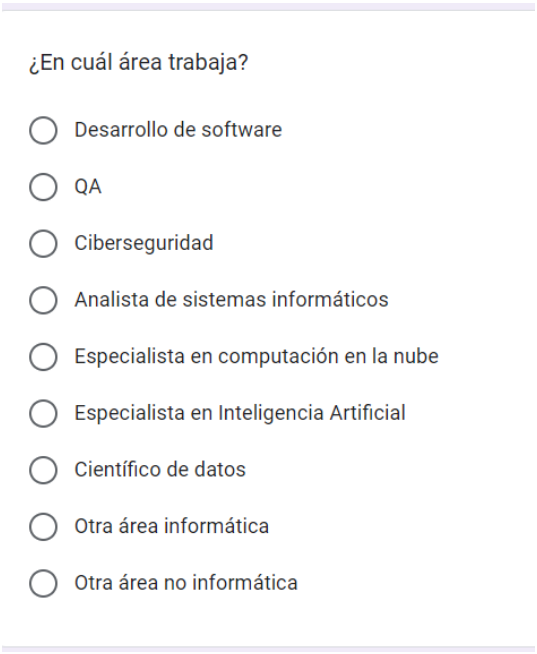

Figura 15: Pregunta n.º 1 de la encuesta

4.4.2 Pregunta n.º 2

¿Aplica buenas prácticas al utilizar/implementar la criptografía en sus actividades diarias? Con opción cerrada de sí o no. El objetivo es identificar el porcentaje de aquellas personas que utilizan buenas prácticas en sus actividades diarias cuando implementan criptografía independientemente de que si emplean o no alguno de los métodos de criptografía.

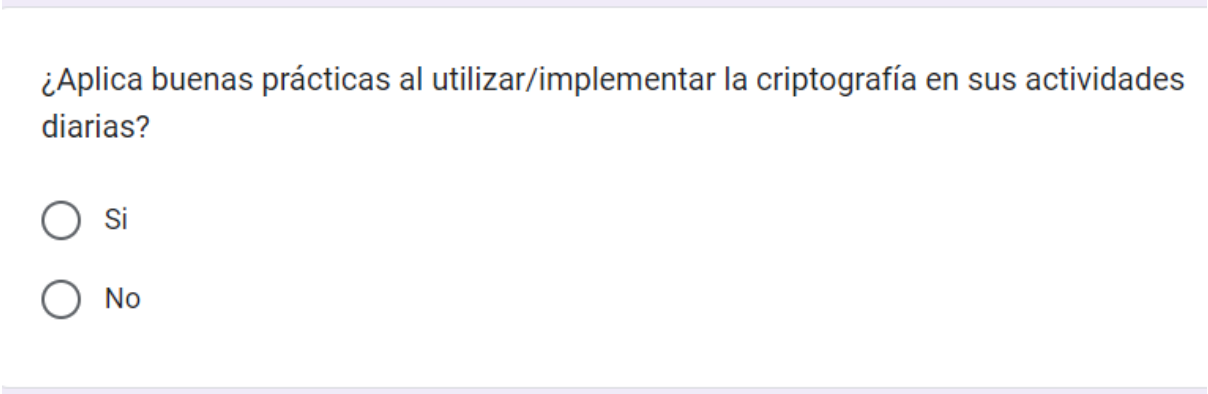

Figura 16: Pregunta n.º 2 de la encuesta

4.4.3 Pregunta n.º 3

¿Utiliza la criptografía para proteger sus datos digitales? Con opción cerrada de sí o no. El objetivo es identificar si las personas, de forma consciente, utilizan la

criptografía para proteger sus datos digitales independientemente sobre si utilizan buenas prácticas en implementación.

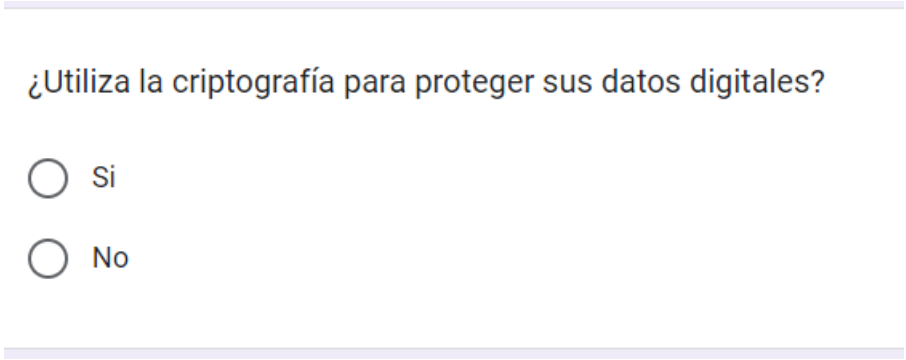

Figura 17: Pregunta n.º 3 de la encuesta

4.4.4 Pregunta n.º 4

¿Podría identificar al menos 7 entornos computacionales en donde puede implementarse la criptografía? Con opciones:

- Sí, identifico los 7 entornos (o más)
- Sí, identifico algunos entornos, pero menos de 7
- No identifico ninguno.

El objetivo es determinar el conocimiento de las personas en cuanto a los entornos computacionales en los cuales la criptografía puede implementarse y, de esta manera, validar la frecuencia y exactitud del uso de la criptografía como método de protección en los diferentes entornos con los que cuentan las arquitecturas y sistemas en la actualidad.

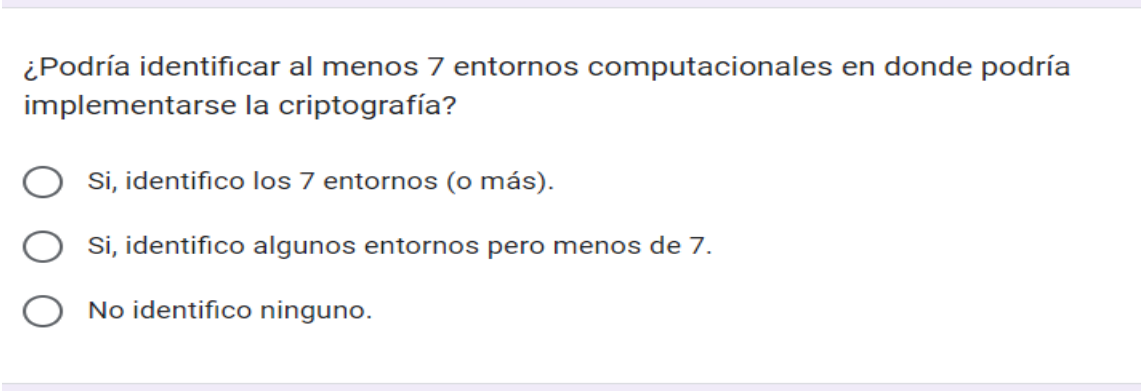

Figura 18: Pregunta n.º 4 de la encuesta.

4.4.5 Pregunta n.º 5

¿Conoce usted qué es criptografía simétrica, asimétrica y curvas elípticas? Con las opciones:

- Sí, conozco sobre criptografía simétrica.
- Sí, conozco sobre criptografía asimétrica.
- Sí, conozco sobre criptografía de curvas elípticas.
- No conozco ninguna.

El objetivo es validar el conocimiento general sobre los métodos de criptografía concernientes a la presente investigación en los diferentes campos de la tecnología y, de esta manera, fundamentar el estudio.

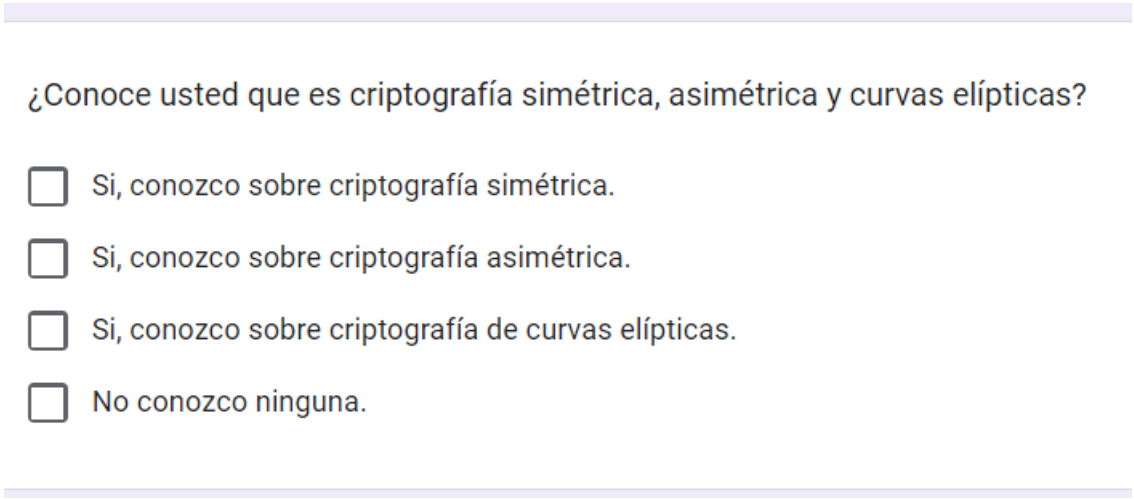

Figura 19: Pregunta n.º 5 de la encuesta

4.4.6 Pregunta n.º 6

¿Conoce usted las ventajas entre criptografía simétrica, asimétrica y curvas elípticas? Con opción cerrada de sí o no. El objetivo es verificar que el uso e implementaciones de los métodos criptográficos se utilicen de manera consciente y acertada y, a la vez, conocer las falencias en cuanto al conocimiento actual en las diferentes áreas tecnológicas.

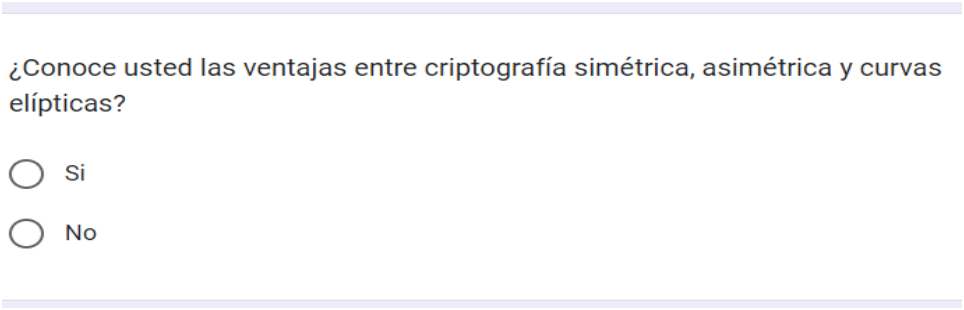

Figura 20: Pregunta n.º 6 de la encuesta

4.4.7 Pregunta n.º 7

¿Podría usted diferenciar la eficacia entre la criptografía simétrica, asimétrica y curvas elípticas? Con opción cerrada de sí o no. Con el objetivo de verificar la forma y usos que se les da a las implementaciones de criptografía y, a la vez, conocer el conocimiento general sobre el nivel de aplicabilidad en cuanto a seguridad por personal informático.

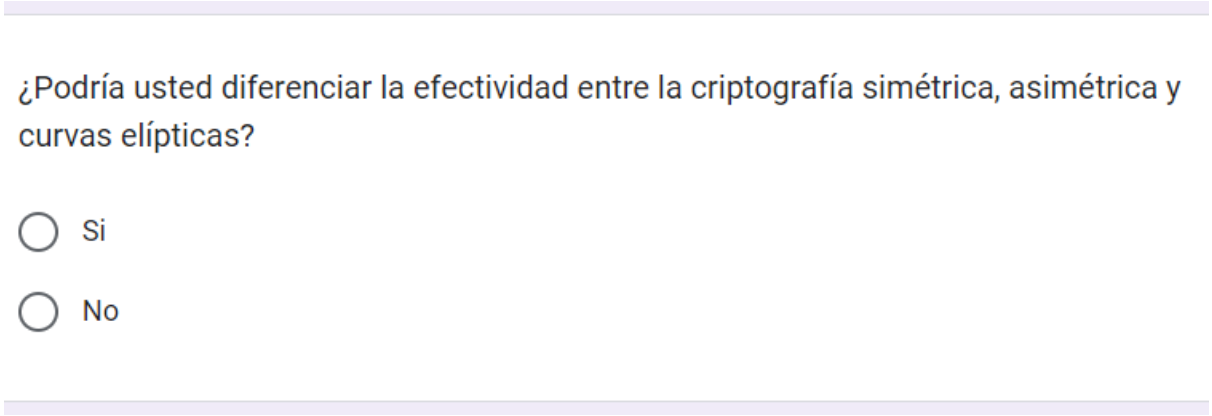

Figura 21: Pregunta n.º 7 de la encuesta

4.5 Resultados

Durante un periodo de 2 semanas se ha podido recopilar el total de 305 respuestas vía la encuesta a través de los medios mencionados.

4.5.1 Resultados pregunta n.º 1

El área con mayor interacción fue la del desarrollo de *software*, la cual se ubica en primer lugar con un indiscutible 54.5 % del total de las personas encuestadas y, por otro lado, con 0 % a las áreas propuesta para especialistas en inteligencia artificial y científico de datos. A continuación, se brindan los datos desglosados:

¿En cuál área trabaja?		
Área	**Porcentaje**	**Encuestados**
Desarrollo de *software*	54.4 %	166
QA	19 %	58
Otra área informática	9.2 %	28
Otra área no informática	8.2 %	25
Analistas de sistemas informáticos	4.3 %	13
Especialistas en computación en la nube	3.6 %	11
Ciberseguridad	1.3 %	4
Especialistas en inteligencia artificial	0 %	0
Científico de datos	0 %	0
Total	**100 %**	**305**

Tabla 17: Desglose de áreas de la primera pregunta de la encuesta

Fuente: Encuesta para la investigación.

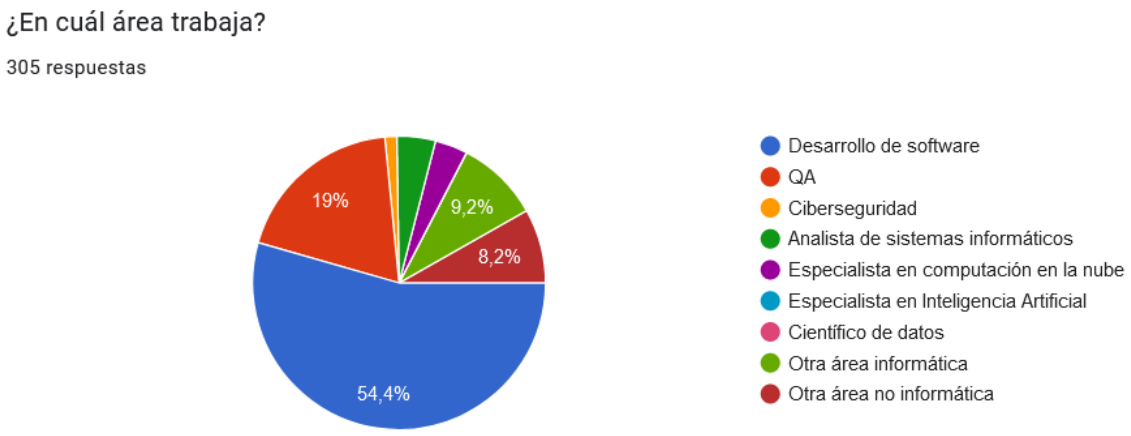

Figura 22: Áreas Encuestadas para la encuesta

Fuente: Encuesta para la investigación.

4.5.2 Resultados pregunta n.º 2

Del total de 305 personas encuestadas, el 59 % expresa que no aplica buenas prácticas al utilizar o implementar la criptografía en sus actividades diarias contra un 41 % que indica que sí aplica en cierta medida buenas prácticas en sus actividades.

Con esto se puede observar que casi un 59 %, casi dos tercios del total de las personas encuestadas, no aplican buenas prácticas y el restante 41 %, quienes indicaron que aplicaban buenas prácticas, queda en tela de duda debido a los resultados que se ven en las siguientes respuestas.

¿Aplica buenas prácticas al utilizar/implementar la criptografía en sus actividades diarias?		
Respuesta	**Porcentaje**	**Encuestados**
No	59 %	180
Sí	41 %	125
Total	**100 %**	**305**

Tabla 18: Desglose de buenas prácticas de la segunda pregunta de la encuesta

Fuente: Encuesta para la investigación.

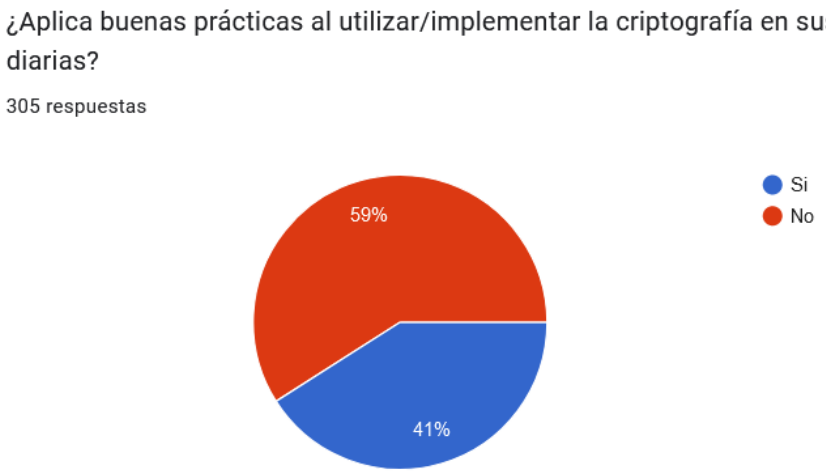

Figura 23: Buenas prácticas implementadas en la encuesta

Fuente: Encuesta para la investigación.

4.5.3 Resultados pregunta n.º 3

Por un lado, se tiene que el 66.9 % indica que en efecto utilizan criptografía para proteger sus datos digitales contra un 33.1 % quienes no la utilizan, al menos de forma consciente. Por otra parte, en cuanto al resultado de la pregunta n.º 2, se puede observar que, aunque más de dos tercios de las personas encuestadas utilizan criptografía en cierta medida, gran porcentaje no utiliza buenas prácticas para implementarlos en sus sistemas. Esto propicia brechas de seguridad con el falso sentimiento de seguridad únicamente por el uso de algún algoritmo criptográfico cualquiera.

¿Utiliza la criptografía para proteger sus datos digitales?		
Respuesta	**Porcentaje**	**Encuestados**
Sí	66.9 %	204
No	33.1 %	101
Total	**100 %**	**305**

Tabla 19: Desglose de uso de criptografía de la tercera pregunta de la encuesta

Fuente: Encuesta para la investigación.

Figura 24: Uso de la criptografía en la encuesta

Fuente: Encuesta para la investigación.

4.5.4 Resultados pregunta n.º 4

El 55.1 % de las personas encuestadas expresa que pueden identificar menos de 7 tipos de entornos en donde la criptografía puede implementarse. Otro 17.4 % expresa que no conocen ningún entorno en su totalidad en el cual la criptografía puede implementarse y un 27.5 % concluye que sí puede identificar 7 o más entornos. Con esto se puede apreciar que el 72.5 % de las personas encuestadas cuenta con pocos conocimientos sobre en cuáles entornos la criptografía debe implementarse para ofrecer seguridad en los datos digitales. Esto revela que la mayor parte de las personas encuestadas no tiene consciencia sobre los sistemas y medios en los que los datos se almacenan, manipulan y transfieren, lo que da como resultado brechas de seguridad, tanto en el ámbito empresarial como personal en el momento de aplicar la criptografía.

¿Podría identificar al menos 7 entornos computacionales en donde puede implementarse la criptografía?		
Respuesta	**Porcentaje**	**Encuestados**
Sí, identifico algunos entornos, pero menos de 7	55.1 %	168
Sí, identifico los 7 entornos (o más)	27.5 %	84
No identifico ninguno	17.4 %	53
Total	**100 %**	**305**

Tabla 20: Desglose de identificación de entornos cuarta pregunta de la encuesta

Fuente: Encuesta para la investigación.

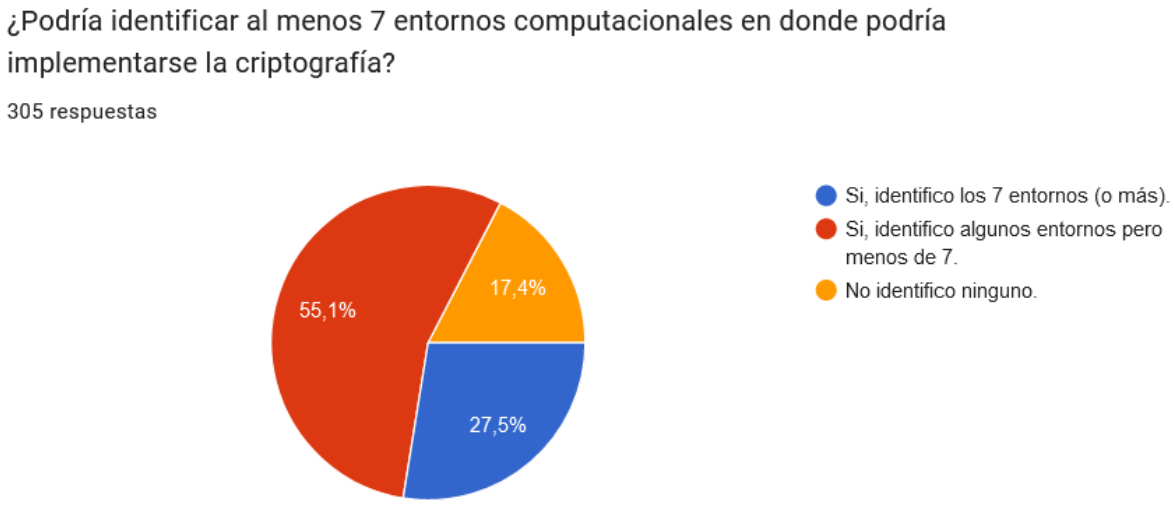

Figura 25: Identificación de entornos en la encuesta

Fuente: Encuesta para la investigación.

4.5.5 Resultados pregunta n.º 5

En cuanto al conocimiento general de las criptografías simétrica, asimétrica y de curvas elípticas, tanto la criptografía simétrica como la asimétrica tienen un gran grado de popularidad entre las personas encuestadas con 73.8 % y 58.7 % respectivamente. No obstante, un gran porcentaje (25.9 %) no conocen los tipos de criptografía presentados. Este porcentaje pertenece a personas con puestos en áreas de la tecnología y, como mínimo se debe tener conocimientos sobre cómo los datos

se tratan para su protección y de esa forma aplicar mejores empleos de estos en el momento de su uso o implementación.

Además, únicamente el 8.5 % de las personas encuestadas expresó haber tenido conocimientos sobre la criptografía de curvas elípticas. Esto tiene sentido, ya que este tipo de criptografía se introdujo hace poco tiempo si se compara con la simétrica y asimétrica como se conocen en la actualidad. No obstante, su teoría tiene varias décadas de existencia, lo que la convierte en una opción bastante sólida con respaldo suficiente para su aplicación como tal.

¿Conoce usted qué es criptografía simétrica, asimétrica y curvas elípticas?		
Respuesta	**Porcentaje**	**Encuestados**
Sí, conozco sobre criptografía simétrica	73.8 %	225
Sí, conozco sobre criptografía asimétrica	58.7 %	179
No conozco ninguna	25.9 %	79
Sí, conozco sobre criptografía de curvas elípticas	8.5 %	26

Tabla 21: Desglose de tipos de criptografía conocidas quinta pregunta de la encuesta

Fuente: Encuesta para la investigación.

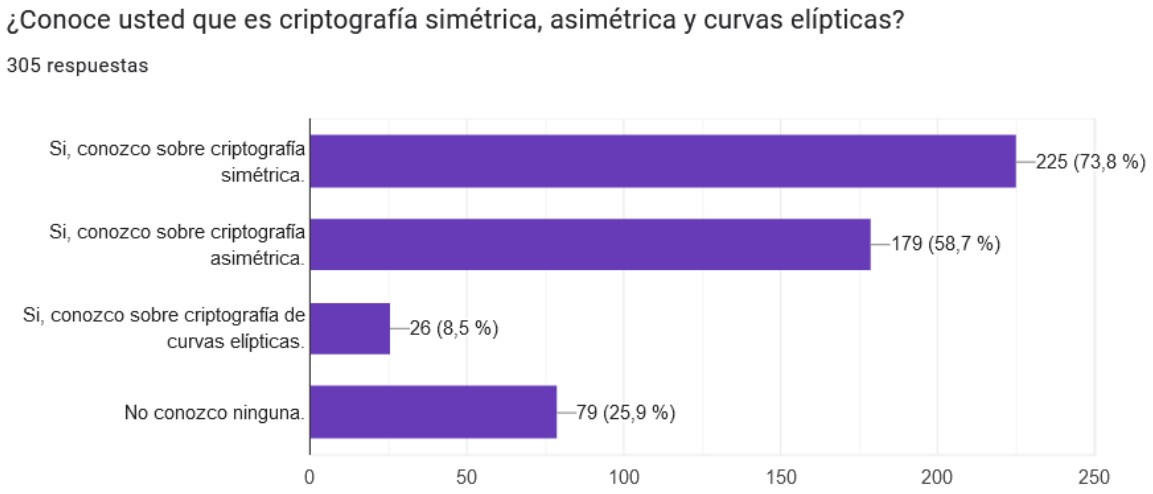

Figura 26: Tipos de criptografía conocidas en la encuesta.

Fuente: Encuesta para la investigación.

4.5.6 Resultados pregunta n.º 6

El 87.9 % de los encuestados declara no conocer las ventajas que constituyen la criptografía simétrica, asimétrica y de curvas elípticas, lo que a la vez demuestra que no solo hace falta implementar la criptografía en los sistemas y medios informáticos, sino que conocer los beneficios que posee cada tipo proporciona mejores resultados, tanto en protección como en recursos de computación necesarios para llevar a cabo la criptografía como tal, lo que reduce tanto costos como tiempo y mejorando la calidad de los servicios que se brindan. Por otro lado, se tiene un 12.1 % quienes afirman conocer las ventajas entre estos tipos de criptografía.

¿Conoce usted las ventajas entre criptografía simétrica, asimétrica y curvas elípticas?		
Respuesta	**Porcentaje**	**Encuestados**
No	87.9 %	268
Sí	12.1 %	37
Total	**100 %**	**305**

Tabla 22: Desglose de ventajas de criptografías sexta pregunta de la encuesta

Fuente: Encuesta para la investigación.

Figura 27: Ventajas de criptografías en la encuesta

Fuente: Encuesta para la investigación.

4.5.7 Resultados pregunta n.º 7

Muy parecido a la situación de las ventajas de las criptografías del punto anterior, se tiene que 88.2 % de las personas encuestadas expresa la carencia de conocimientos para diferenciar la eficacia entre las criptografías simétricas, asimétricas y de curvas elípticas. Esto desemboca en una mezcla entre desconocimiento de las ventajas con desconocimiento de la eficacia de los tipos de criptografías abordados, lo que evidencia la falta de educación en cuanto a seguridad informática con las que cuenta parte del personal en las diferentes áreas de la informática.

¿Podría usted diferenciar la eficacia entre la criptografía simétrica, asimétrica y curvas elípticas?		
Respuesta	**Porcentaje**	**Encuestados**
No	88.2 %	269
Sí	11.8 %	36
Total	**100 %**	**305**

Tabla 23: Desglose de eficacia de criptografías séptima pregunta de la encuesta

Fuente: Encuesta para la investigación.

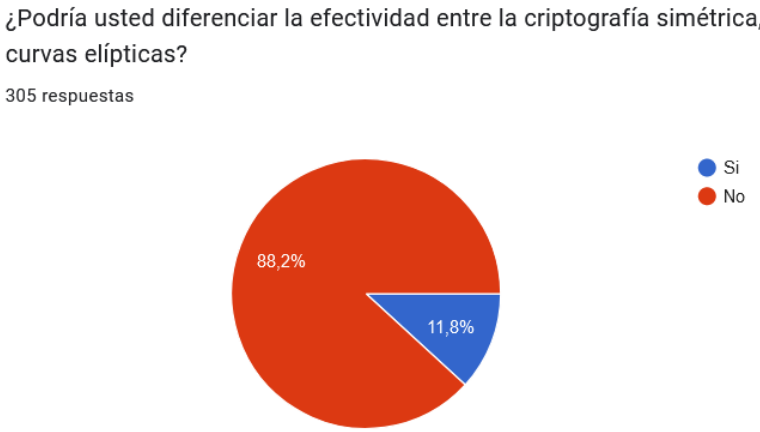

Figura 28: Eficacia de criptografías en la encuesta

Fuente: Encuesta para la investigación.

4.6 Conclusión de los resultados

A través del análisis de los resultados se puede concluir que parte de los profesionales en las diferentes ramas de la informática tienen conocimientos limitados o incluso nulos con respecto al tema de la criptografía y el objetivo que esta tiene en

el ámbito tecnológico actual y la necesidad de su utilización para proteger los datos digitales dentro de cualquier entorno digital.

La mayor parte de la población que compone la encuesta son desarrolladores de *software* seguidos de QA y analistas de sistemas informáticos, los cuales, por su importancia en las empresas (cuyas labores son tan diversas e incluyen el análisis, desarrollo, implementación y mantenimiento de sistemas computacionales) deben poseer conocimientos más amplios sobre el tema de la criptografía para proveer sistemas más seguros desde los primeros pasos del desarrollo de estos sistemas. De esa manera, cubrir en mayor grado las vulnerabilidades que se puedan presentar.

Además del total de profesionales, más de la mitad indica que, en efecto, utilizan criptografía para proteger sus datos digitales, pero, por otra parte, dos tercios de los mismos profesionales declaran no utilizar buenas prácticas al implementar criptografía en sus actividades diarias. Esto se traduce en una falsa sensación de seguridad, lo que produce áreas con grandes posibilidades que contengan vulnerabilidades que pueden explotar cibercriminales.

Aunado al texto anterior, estos profesionales declaran conocer limitados entornos en donde la criptografía puede estar presente para salvaguardar la integridad, confidencialidad y la disponibilidad de los datos digitales. Actualmente estos se utilizan en cualquier ámbito entre los sistemas y redes computacionales, lo que confirma la falsa sensación de seguridad que se ha mencionado hasta el momento.

Además, al igual que cualquier ámbito tecnológico, la criptografía y su implementación en los entornos computacionales también evoluciona para satisfacer las necesidades y requerimientos empresariales y legales con los que algunas empresas deben equipar y sus sistemas y servicios para considerarse seguros. Sin embargo, aproximadamente dos tercios de los profesionales afirman tener familiaridad con la criptografía simétrica y cerca de la mitad con la criptografía asimétrica y solo el 8.5 % expresa conocer la criptografía de curvas elípticas. Lo más preocupante es que el 25.9 % de los profesionales declara no conocer ninguno de los tres tipos de criptografías que se estudian en esta investigación, lo cual ocasiona un panorama en el cual incluso los profesionales dentro de la informática desconocen temas tan importantes para proteger la información. Lo anterior produce el crecimiento

de forma inintencionada del área de ataque para los ciberdelincuentes y pone en riesgo la privacidad de los datos de la población en general.

Lo anterior se puede explicar con el desconocimiento del 88.2 % de los profesionales quienes indican que no logran reconocer de forma explícita las diferencias entre las criptografías simétrica, asimétrica y de curvas elípticas. Además, se confirma en que también el 87.9 % desconoce las ventajas que estas criptografías ofrecen para protección de los datos.

De esta manera, se tiene un panorama mucho más claro en cuanto al tema de la criptografía y el conocimiento que poseen los profesionales en la actualidad, para las implementaciones que se realizan a diario para brindar los servicios que posiblemente se hayan utilizado en algún momento a través de sus plataformas de servicios.

4.7 Análisis documental

Con base en los resultados a través de la encuesta se concreta un panorama mucho más amplio con respecto a la situación actual del conocimiento e implementaciones de la criptografía en los sistemas y usos cotidianos. La carencia de conocimientos de seguridad informática en las distintas áreas de la informática propicia la falsa sensación de seguridad, tanto de forma personal como entre las empresas. Esto puede transformarse en grandes brechas de seguridad debido a que se expone información confidencial o sensible a terceros, lo que conlleva a una posición bastante desfavorable en cualquier ataque.

Además, no es suficiente aplicar criptografía si estas implementaciones no propician las mejores prácticas que brindan grandes organizaciones internacionales cuyos propósitos es la de asegurar la información en los medios digitales en la actualidad. Por lo tanto, resulta necesario brindar más herramientas de forma unificada a la población informática para que el resguardo de la información se aplique de manera adecuada y brinde los resultados que se esperan.

Por este motivo, se determina la viabilidad para el desarrollo del modelo de selección de algoritmos criptográficos modernos simétricos y asimétricos incluyendo curvas elípticas aprobados en entornos informáticos.

Capítulo 5. Propuesta de solución

A través de la observación obtenida durante el análisis de resultados se puede resaltar que muchos profesionales no tienen claro el propósito y las ventajas que ofrecen los algoritmos criptográficos presentados en el momento de usarlos para proteger la información digital. Esto genera una gran incertidumbre en cuanto a la gestión de esta protección realizada en los proyectos y sistemas en los cuales se emplean y ofrecen estos servicios al público, quienes son los que ingresarán los datos para usar estos procesos que se ofrecen.

A continuación, se desarrolla la propuesta de ciberseguridad para gestión y selección de los algoritmos criptográficos modernos simétricos y asimétricos incluyendo curvas elípticas para su aplicación en los entornos computacionales.

Para fundamentar el objetivo del presente documento se han tomado las publicaciones especiales y documentos de estándares internacionales de NIST y FIPS. La presente propuesta toma en cuenta únicamente aquellas partes de los documentos que al investigador le han parecido pertinentes a través del análisis de los actuales estándares y normativas internacionales, sin embargo, no es necesario que se utilice como marco de referencia para implementaciones o, en su defecto, para cumplir con estos estándares y normativas. Por lo tanto, cada organización está obligada a cumplir con los temas legales alrededor del área de negocio u operación en sus países.

Debido a que la investigación no tomó la completitud de temas que se relacionan con los procesos criptográficos, los cuales pueden verse reflejados en algunos casos especiales, cada entidad está en la obligación de consultar los estándares o normas no evaluadas para la presente propuesta cuando sea requerido.

Finalmente, la persona investigadora hará referencia a documentos y estándares de NIST y FIPS durante el desarrollo de la propuesta. Por lo tanto, se recomienda la revisión y evaluación de estos documentos oficiales para profundizar cada uno de los temas requeridos por las distintas organizaciones en temas que se relacionan con procesos criptográficos para una implementación adecuada.

Cabe destacar que la presente propuesta tiene como objetivo servir como guía inicial para la selección de algoritmos criptográficos seguros de forma estándar para cualquier organización. Por consiguiente, si se requieren temas más a fondo se

recomienda la lectura de las publicaciones de NIST y FIPS en su totalidad en sus versiones más actualizadas.

Se utiliza como referencia principal las publicaciones especiales de NIST 800-175B Revisión 1 (Guideline for Using Cryptographic Standards in the Federal Government) y 800-57 Part 1 Revision 5 (Recommendation for Key Management) de los cuales se desprende el siguiente modelo de la propuesta:

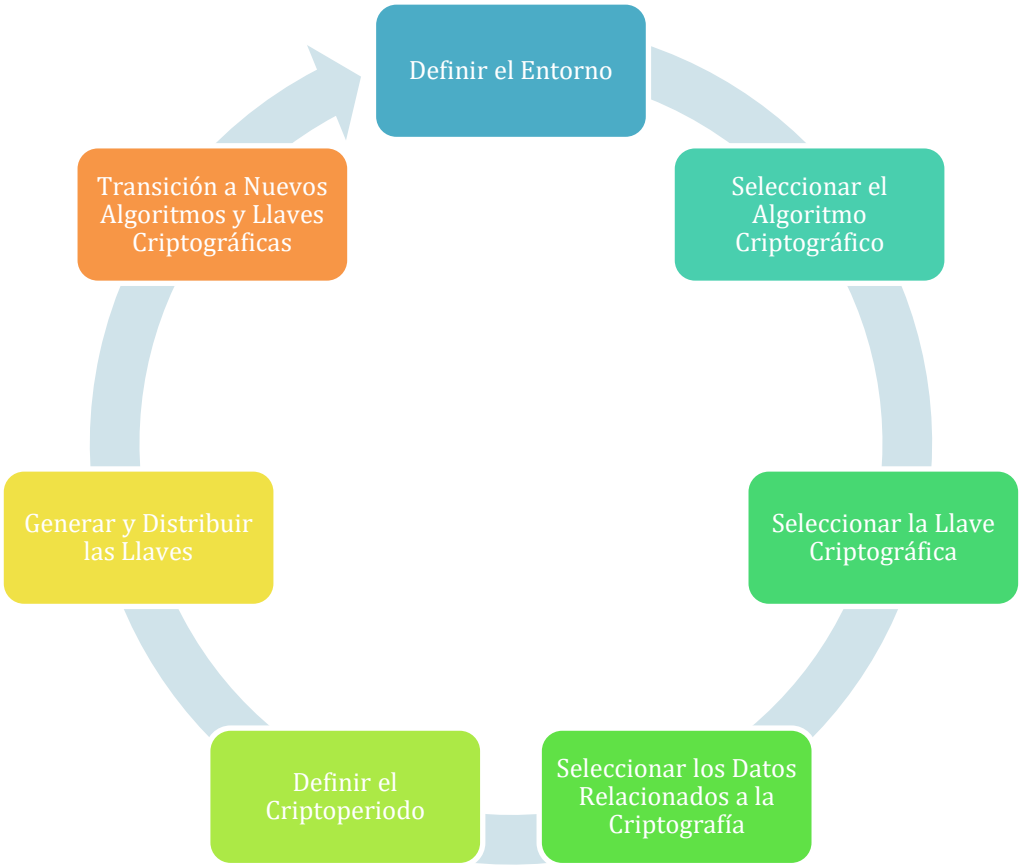

Figura 29: Diagrama del modelo de selección

Fuente: Publicación especial de NIST SP 800-175B Revisión 1

En el diagrama anterior se observa que para la propuesta del modelo de selección de los algoritmos criptográficos es necesario cumplir con siete pasos, los cuales detallan las etapas que se deben tomar en cuenta para decidir el fin y el tipo de seguridad que se requiera implementar a través de la criptografía.

5.1 Definir el entorno

Como primer paso a la protección de los datos digitales se debe analizar lo que se desea proteger y el estado en que permanecerán estos datos mientras se

protegen. A continuación, se brinda un listado de entornos populares en donde la criptografía desempeña un papel fundamental para la protección de la integridad, confidencialidad y disponibilidad de los datos.

Figura 30: Entornos informáticos

5.1.1 Estado de los datos

Se debe definir el estado en el que los datos que se desean proteger permanecerán. De esta manera, se encaminan la selección del algoritmo criptográfico que mejor se ajuste a la necesidad presentada.

Figura 31: Estados de los datos

Fuente: SealPath (2022).

5.1.2 Estado en reposo

Los datos en reposo son aquellos que se encuentran en un único lugar en un momento determinado, es decir, no se encuentran ni en tránsito ni en uso. Esto lo convierte en un objetivo atractivo para los actores malintencionados, así se puede listar algunos posibles escenarios en donde los datos puedan estar en este estado:

- Servidor de archivos
- Estación de trabajo
- Base de datos
- Pendrive
- En la nube
- Disco duro
- CD-ROM

Antes de aplicar cualquier medida de seguridad, la organización debe ser capaz de responder a las siguientes preguntas, con el fin de poseer conocimientos sobre sus propios datos y así aplicar la mejor protección:

1) ¿En dónde residen los datos?
2) ¿Cómo están clasificados los datos? (nivel de sensibilidad)
3) ¿Cuál es el formato de los datos?
4) ¿Quién tiene/requiere acceso a los datos?

5.1.2.1 Disponibilidad

Se lleva a cabo a través de:

- Copias de la información encriptada separadas en diferentes ubicaciones.
- Almacenamiento operacional normal o almacenamiento tipo *backup*.
- Datos encriptados después de la caducidad del criptoperiodo de la llave deben archivarse.

5.1.2.2 Integridad

Se obtiene a través de mecanismos físicos o criptográficos (o ambos):

1) Mecanismos físicos:
   - Sistema operativo o módulo criptográfico válido que limite el acceso a los datos almacenados.
   - Sistema o medio computacional que no esté conectado con otros sistemas.

- Ambientes físicos seguros con accesos apropiados a los datos almacenados y que no se encuentre conectado con los sistemas computacionales en uso.

2) Mecanismos criptográficos:
   - Mecanismos de integridad aprobados usados para computar sobre la información clave y, posteriormente, se utiliza para verificar la integridad de información clave.
   - Usar operaciones criptográficas cuyo resultado se considera correcto y si el destinatario no puede validar el mismo resultado entonces se considera corrupto.

5.1.2.3 Confidencialidad

Se lleva a cabo a través de los siguientes mecanismos:

- Encriptación con algoritmos aprobados.
- Agregar protección física. Ver FIPS 140 (módulos criptográficos válidos).
- Proveer protección física con controles de acceso a los datos almacenados.

5.1.3 Estado en tránsito

En este estado los datos se encuentran siendo transferidos de un punto a otro, por lo tanto, se traslada por canales probablemente inseguros a través de todo Internet. Por este motivo, es necesario implementar medidas adecuadas para que los datos continúen con la confidencialidad, integridad y disponibilidad requerida.

5.1.3.1 Disponibilidad

Debido a que las comunicaciones pueden alterarse o destruirse intencionalmente, solo utilizar criptografía no es suficiente. Por lo tanto, se deben utilizar otros mecanismos como la redundancia, canales múltiples, sistemas de almacenamiento y reenvío, códigos de corrección de errores y otros mecanismos no criptográficos para llevar a cabo este tipo de tarea.

5.1.3.2 Integridad

Abarca los temas que se relacionan con prevenir y detectar modificaciones en la información. Para asegurarse de que la información no ha sido alterada se necesita uno o más de los siguientes mecanismos:

1) Método manual
    - Generar un código (CRC, MAC, firma digital, *hash*) que es compartido con el destinatario, el cual debe saber las llaves y mecanismos para generar y verificar este código. Si el resultado es el mismo entonces la información no ha sido alterada.
    - Enviar tanto la llave como la información encriptada (conocida por ambos) al destinatario, si puede reversar o verificar la operación criptográfica que utiliza el emisor usando la llave compartida para desencriptar la información conocida por ambos entonces esta se asume inalterada.
2) Distribución automatizada vía protocolos de comunicación (protección proveída por en emisor o el propio protocolo de comunicación)
    - Utilizar un mecanismo de integridad criptográfica aprobada para generar un código sobre la información encriptada, el cual es proveído al destinatario para su verificación. El mecanismo de integridad puede aplicarse únicamente en información clave o en todo el mensaje.
    - Tanto la llave como la información clave las usa el emisor para ejecutar la operación criptográfica sobre la información. Después, tanto la llave como la información protegida se envía al destinatario y, si este puede reversar o verificar la operación criptográfica que se utiliza entonces puede haber seguridad de que no ha sido alterada.
3) Confidencialidad

    Se presenta a través de las llaves simétricas, llave privada del par de llave asimétrico, compartición de llave y metada secreta usando:
    - Algoritmos y llaves de encriptación aprobadas.
    - Mecanismos para dividir la llave en múltiples partes.
    - Protección apropiada, tanto para los procedimientos como para la parte física.

- Encriptando la propia llave usando otra técnica de encriptación aprobada.

5.1.4 Estado en uso

Al igual que en los otros estados, se necesita mantener la confidencialidad, integridad y disponibilidad de los datos, con la diferencia de que en este estado los datos se utilizan en las operaciones de la lógica del negocio. Estos se encuentran almacenados en memoria no persistente como en la memoria de acceso aleatorio (RAM), la caché de la CPU o en los propios registros en cuanto los dispositivos computacionales los usan de forma activa.

Se debe tener en cuenta que los datos en uso son particularmente difíciles de encriptar debido a que se encuentran siendo procesados de forma activa. Por lo tanto, la encriptación puede afectar el rendimiento e incluso se puede llegar a la situación en donde el procesamiento se vuelva imposible.

Debido a lo anterior, se aconseja realizar las operaciones del negocio en ambientes protegidos con el endurecimiento apropiado, según sea necesario como corresponda en cada caso en particular.

5.2 Seleccionar el algoritmo criptográfico

La elección del algoritmo debe basarse en los requerimientos de la empresa, el entorno y los estados en los que se presentan los datos. Para aclarar el panorama, se muestran a continuación las características más relevantes sobre la criptografía simétrica y asimétrica incluyendo curvas elípticas, además de los algoritmos de *hash*.

5.2.1 Características

La encriptación de datos en su definición más simple es el proceso de transformar datos desde su formato original inteligible a un nuevo formato ininteligible. A continuación, se detallan los algoritmos simétricos y asimétricos incluyendo curvas elípticas aprobados por NIST.

5.2.2 Algoritmos Simétricos

A continuación, se detallan las características de los algoritmos aprobados por NIST hasta la fecha de esta investigación.

5.2.2.1 Usos

Los algoritmos de llave simétrica se utilizan para:

- Cifrado y descifrado para garantizar la confidencialidad de los datos utilizando la misma llave.
- Autenticación para garantizar la integridad de los datos y su fuente.
- Autenticación e integridad de los servicios a través de MAC (código de autenticación de mensaje); la llave se utiliza para generar y validar el MAC.
- Derivación de material clave de llaves precompartidas utilizando métodos de derivación de llaves.
- Derivación de llaves desde un secreto compartido durante un esquema de acuerdo de llaves asimétricas.
- Envoltura de la llave.
- Generación de bits aleatorios.

5.2.2.2 Detalles

- Conocidos como algoritmos de llave secreta.
- Se utiliza la misma llave, tanto para encriptar como para desencriptar.
- Por cada par de entes se debe generar una llave diferente.
- Los algoritmos de llave secreta tienden a ser más rápidos que los algoritmos de llave pública.
- Las llaves son más cortas para la misma fuerza de seguridad con respecto a las de llaves de los algoritmos de llave pública.

5.2.2.3 Algoritmos simétricos aprobados

Algoritmos simétricos con base en cifrado por bloques	
Algoritmo	**Descripción**
AES "Advanced Encryption Standard" (estándar de encriptación avanzada)	Además, conocido como Rijndael, se desarrolló como sucesor, tanto de DES como de TDEA. Es el algoritmo de cifrado por bloque preferido para los nuevos productos. Utiliza llaves criptográficas con longitudes de 128, 192 y 256 bits para encriptar y desencriptar en bloques simétricos de entrada y salida de 128 bits (estos son los aceptados por el estándar actual). Los números de rondas realizadas en cada ejecución dependen del tamaño de la llave, así se tiene que: * Llave de 128 bits = 10 rondas * Llave de 192 bits = 12 rondas * Llave de 256 bits = 14 rondas

Tabla 24: Algoritmos simétricos con base en cifrado por bloques

Fuente: FIPS 197 Announcing the Advanced Encryption Standard (AES).

Algoritmos simétricos con base en funciones hash	
Abreviación de la función	**Descripción**
CSHAKE "Customable version SHAKE" (versión personalizable de SHAKE)	Es una versión personalizable del algoritmo SHAKE, la cual incluye una nueva entrada de tipo cadena personalizable, la cual trabaja como nombre de la función para computar diferentes resultados utilizando diferentes valores. En caso de que no se desee esta personalización entonces la

	cadena de entrada se establece como una cadena vacía. Existen dos variantes: * cSHAKE128: Resultado de salida de 128 bits. * cSHAKE256: Resultado de salida de 256 bits.
KMAC "KECCAK Message Authentication Code" (código de autenticación de mensaje KECCAK)	Es una función *hash* con llave de longitud variable y se le conoce por ser una función pseudoaleatoria. Su núcleo se basa en SHA-3. Existen dos variantes: * KMAC128: Llave de longitud de 128 bits y resultado de salida de 256 bits. * KMAC256: Llave de longitud 256 y resultado de salida de 512 bits. En teoría, este algoritmo puede producir flujos de *bytes* infinitamente largos. El resultado de salida de KMAC puede extenderse hasta una longitud deseada a través de si se usa como un XOF (*eXtendable Output Functions*) o función de salida extendida.
TupleHash "Tuple Hash" (tuplas de *hash*)	Es una función *hash* derivada en SHA-3 con salida de longitud variable, la cual está diseñada para crear un *hash* a partir de una tupla de cadenas de entrada. Esta tupla consiste en una cantidad de cadenas (lo que incluye cero), la cual se representa como una secuencia de

	entradas o variables como (“a”, b, “c”, “d”... “z”). Este algoritmo soporta llaves tanto de 128 bits como de 256 bits. El cambio de cualquier parámetro de entrada de la función, lo que incluye la longitud de salida solicitada, resulta en un cambio casi con seguridad de la salida final. Este algoritmo puede usarse como XOF (eXtendable Output Functions) o función de salida extendida, lo cual permite imitar el comportamiento de cSHAKE, lo que incluye el resultado de longitud infinita.
ParallelHash “Parallel Hash” (*hash* paralelo)	El objetivo de esta función es la de dar soporte a los procesos de *hash* de cadenas de grandes longitudes de forma eficiente a través de los mecanismos de paralelismo de los procesadores modernos. Soporta llaves de 128 y 256 bits con salidas de longitudes variables. El cambio de cualquier parámetro de entrada de la función, lo que incluye la longitud de salida solicitada, resulta en un cambio completamente diferente de la salida final. Además, soporta cadenas personalizables definidas por la persona usuaria. Este algoritmo puede usarse como XOF (*eXtendable Output Functions*) o función de salida extendida, lo cual permite

	imitar el comportamiento de cSHAKE, lo que incluye el resultado de longitud infinita.

Tabla 25: Algoritmos simétricos con base en funciones hash
Fuente: NIST Special Publication 800-185 y FIPS PUB 186-4.

5.2.3 Algoritmos asimétricos

5.2.3.1 Usos

Los algoritmos de llave asimétrica se usan para:

- Proporcionar servicios de identidad, integridad y autenticación de fuentes en forma de firmas digitales.
- Establecer material de clave criptográfica utilizando algoritmos de acuerdo y transporte de llaves.

5.2.3.2 Detalles

- Se conocen también como algoritmos de llave pública.
- Se utilizan dos llaves, la privada (encriptar) y la pública (desencriptar) o viceversa.
- La llave privada debe mantenerse en secreto mientras la pública puede compartirse entre diferentes entidades.
- La llave privada no puede determinarse a través de la llave pública ni al contrario.
- Los algoritmos de llave pública tienden a ser más lentos que los de llave secreta.
- No suelen utilizarse en procesos de criptografía de grandes volúmenes de datos.
- Puede combinarse el uso con criptografía simétrica cuando se realiza el proceso de establecimiento de llave, lo cual mejora la eficiencia porque reduce el número de llaves requeridas.
- Las claves son más largas para la misma fuerza de seguridad con respecto a las de llaves de los algoritmos de llave secreta.
- Después del cambio a la computación cuántica, los algoritmos de llave pública no proveerán una protección adecuada.

- Adecuado para ambientes abiertos o multiusuarios.

5.2.3.3 Algoritmos asimétricos aprobados

Algoritmos asimétricos de firma digital	
Nombre	Descripción
DSA "Digital Signature Algorithm" (algoritmo de firma digital)	Se utiliza para generar y verificar firmas digitales usando campos finitos. FIPS 186 determina los métodos para generar los parámetros de dominio, pareja de llaves y longitudes de llaves para validar la seguridad en la generación y verificación que se brinda en los procesos de firma digital. Requiere más tiempo de cómputo para realizar los procesos criptográficos en comparación con RSA, ECDSA y EdDSA. La fuerza de seguridad de la función *hash* que se utiliza en los procesos criptográficos debe ser igual o superior a la fuerza de seguridad que brinda el conjunto (L, N). La norma de FIPS 186-4 especifica las siguientes opciones para el par L y N (las longitudes de bits de p y q, respectivamente): $L = 1024, N = 160$ $L = 2048, N = 224$ $L = 2048, N = 256$ $L = 3072, N = 256$
ECDSA "Elliptic Curve Digital Signature Algorithm" (algoritmo de firma digital de curva elíptica)	Es una variante de DSA. Tanto el algoritmo de verificación como de firma básica son iguales a los de DSA, con la diferencia de que, en lugar de utilizar la matemática de campos finitos,

	ECDSA utiliza curvas elípticas con problemas de logaritmos discretos. Posee longitudes de llaves mucho más cortas, lo que permite utilizar menos espacio de almacenamiento y ancho de banda para la transmisión, por lo que es conveniente en entornos con recursos limitados, lo que incluye el consumo de energía. La ejecución del algoritmo es más rápida al utilizar menos poder de computación para calcular la llave. Posee llaves considerablemente más cortas que las de RSA y la ejecución del algoritmo es mucho más rápido por el mismo hecho. Posee un *nonce* aleatorio, el cual se crea en el proceso de creación de la firma y, se debe asegurar que este no se reutilice para el siguiente proceso. Las firmas de ECDSA cambian en cada proceso debido al *nonce* que es diferente por cada proceso incluso y tiene los mismos parámetros del proceso anterior. ANS X9.62 define métodos para la generación y verificación de firmas para ECDSA. La seguridad proveída por este algoritmo es:

Longitud de bits de *n* (llave)	**Cofactor máximo *h* (que es igual al orden de la curva dividido por *n*)**
224-255	2^{14}
256-383	2^{16}
384-511	2^{24}
≥ 512	2^{32}

Además, se muestran las longitudes de bits de los campos subyacentes de las curvas que se recomiendan:

Longitud de bits de "n"	**Campos primos**	**Campos binarios**
224-255	Len(p) = 224	M = 233
256-383	Len(p) = 256	M = 283
384-511	Len(p) = 384	M = 409
≥ 512	Len(p) = 521	M = 571

Las curvas elípticas que se recomiendan por NIST SP 800-186 para este algoritmo son:

Curvas Weierstrass	**Curvas Montgomery**	**Curvas Edwards25519**
P-224	Curve25519	Edwards448
P-256	Curve448	E448
P-384	-	-
P-521	-	-
W-25519	-	-
W-448	-	-

Las curvas que se recomiendan para ECDSA se proveen en el Apéndice A.

Para generar una firma digital de ECDSA se debe contar con lo especificado en ANS X9.62:

	1) Definir el dominio de parámetros. 2) Definir la llave privada. 3) Obtener un número secreto por mensaje que se genera. 4) Utilizar una función de *hash* aprobada. 5) Utilizar un generador de *bits* aleatorios para la llave privada.
EdDSA "Edwards-curve Digital Signature Algorithm" (algoritmo de firma digital de la curva de Edwards)	Las firmas de EdDSA son terministas, es decir, el valor único de la llave se computa usando la llave privada y el propio mensaje por firmarse, lo que produce aleatoriedad suficiente para evitar ataques. Por lo tanto, no se requiere un generador aleatorio de *bits* para su creación, sin embargo, FIPS 186-5 recomienda su uso utilizando RBG aprobados. Es más nueva que ECDSA y mejora tanto el rendimiento como la seguridad. No utiliza un *nonce* aleatorio como ECDSA, por lo tanto, para los mismos parámetros de entrada se obtiene el mismo resultado. El IETF RFC-8032 recomienda los parámetros para las curvas Ed25519 (edwards25519) y Ed448 (edwards448) que utiliza el algoritmo. La fuerza de seguridad proveída por Ed25519 es de 128 bits mientras que la de Ed448 es de 224 bits. La llave púbica de Ed25519 es de 256 bits mientras que la de Ed448 es de 456 bits.

<table>
<tr><td></td><td>La función criptográfica hash para generar llaves para Ed25519 es SHA-512 mientras que para Ed448 es SHAKE256.
HashEdDSA “Prehash Edwards-Curve Digital Signature Algorithm” (algoritmo de firma digital Prehash Edwards-Curve) es una versión de EdDSA cuya mayor diferencia es que genera una firma basada sobre el hash del mensaje mientras que EdDSA firma el mensaje directamente, lo que produce que deba realizar el proceso de hash dos veces mientras HashEdDSA lo hace una única vez.
No obstante, el dominio de parámetros y la generación de llaves, tanto HashEdDSA como EdDSA son exactamente los mismos.</td></tr>
<tr><td>RSA (Rivest, Shamir y Adleman)</td><td>FIPS 186 determina las restricciones correspondientes para el uso de RSA en donde se incluyen la generación del par de llaves, métodos y longitud de llaves.
Para RSA, se recomiendan longitudes de llaves de:
<table>
<tr><th>Longitud de llave</th><th>Fuerza de seguridad</th></tr>
<tr><td>2048</td><td>112</td></tr>
<tr><td>3072</td><td>128</td></tr>
<tr><td>4096</td><td>152</td></tr>
<tr><td>6144</td><td>176</td></tr>
<tr><td>8192</td><td>200</td></tr>
</table>
</td></tr>
</table>

	Si se usa una función *hash* en el proceso de generación de llaves esta debe proveer bloques de salida para cumplir o superar la fuerza de seguridad requerida para el proceso de firma digital de RSA. Los valores que se utilizan para generar las llaves de RSA deben ser el resultado de una función RBG. NIST 800-56B revisión 2 recomienda utilizar RSASVE (RSA Secret-Value Encapsulation) o SA-OAEP (RSA with Optimal Asymmetric Encryption Padding) para procesos de encriptación/desencriptación de RSA. RSA realiza los procesos criptográficos más rápido que DSA.

Tabla 26: Algoritmos asimétricos de firma digital

Fuente: NIST SP 800-56B Revision 2 y FIPS PUB 186-5

Algoritmos asimétricos de esquemas de establecimiento de llaves	
Nombre	**Descripción**
DH (Diffie−Hellman)	Se utiliza para el intercambio de llaves entre entidades a través de entornos inseguros (como Internet). Generalmente, se emplea para los acuerdos de llaves simétricas. Las llaves que se generan se utilizan típicamente por cortos periodos y después pasan a descartarse para generar otro conjunto nuevo de llaves. Por eso, se les conoce como llaves efímeras.

DH usa primitivas de DLC conformadas por dos conjuntos: FFC (FFC DH) y ECC (ECC DH).

Curvas elípticas aprobadas para el acuerdo de llaves de ECC DH:

Curva	**Fuerza de seguridad soportada**
P-224	S = 112
P-256	$112 \leq s \leq 128$
P-384	$112 \leq s \leq 192$
P-521	$112 \leq s \leq 256$
K-233	$112 \leq s \leq 128$
K-283	$112 \leq s \leq 128$
K-409	$112 \leq s \leq 192$
K-571	$112 \leq s \leq 256$
B-233	$112 \leq s \leq 128$
B-283	$112 \leq s \leq 128$
B-409	$112 \leq s \leq 192$
B-571	$112 \leq s \leq 256$

Los grupos de números primos seguros para acuerdo de llaves para FFC DH:

Grupo	**Longitud de bits de la llave**	**Fuerza de seguridad soportada**
14	2048-bit	S = 112
15	3072-bit	$112 \leq s \leq 128$
16	4096-bit	$112 \leq s \leq 152$
17	6144-bit	$112 \leq s \leq 176$
18	8192-bit	$112 \leq s \leq 200$

MQV (Menezes-Qu-Vanstone)	Es una variante del algoritmo Diffie-Hellman. Puede emplear criptografía de campos finitos a través de los esquemas MQV1 y MQV2. Posee una variación que emplea curvas elípticas denominada ECMVQ (Véase “algoritmos asimétricos de curvas elípticas”). Al igual que DH, sus llaves también se dedican para el intercambio de llaves entre entidades a través de entornos inseguros (como Internet). Generalmente, se emplea para los acuerdos de llaves simétricas. Las llaves que se generan se utilizan típicamente por cortos periodos y después pasan a descartarse para generar otro conjunto nuevo de llaves. Por eso, se le conocen como llaves efímeras. Los pasos para el proceso de acuerdo de llave son igual, tanto para DH como para MQV: 1. Generación de parámetros de dominio 2. Intercambio de parámetros de dominio 3. Validación de parámetros de dominio 4. Generación de claves privadas y públicas 5. Comunicación de las claves públicas 6. Validación de las claves públicas 7. Cálculo de los números secretos compartidos

<table>
<tr><td></td><td>8. Derivación de la clave a partir de los números secretos compartidos
9. Uso de la clave derivada
Las llaves que se recomiendan para MQV son las siguientes:
<table><tr><th>Grupo</th><th>Longitud de bits de la llave</th><th>Fuerza de seguridad soportada</th></tr><tr><td>14</td><td>2048-bit</td><td>S = 112</td></tr><tr><td>15</td><td>3072-bit</td><td>112 ≤ s ≤ 128</td></tr><tr><td>16</td><td>4096-bit</td><td>112 ≤ s ≤ 152</td></tr><tr><td>17</td><td>6144-bit</td><td>112 ≤ s ≤ 176</td></tr><tr><td>18</td><td>8192-bit</td><td>112 ≤ s ≤ 200</td></tr></table></td></tr>
<tr><td>RSA (Rivest, Shamir y Adleman)</td><td>Véase “algoritmos asimétricos de firma digital”</td></tr>
</table>

Tabla 27: Algoritmos asimétricos de esquemas de establecimiento de claves

Fuente: NIST SP 800-56 A Revision 3, NIST SP 800-56B Revision 2 y RFC-3526

Algoritmos asimétricos de curvas elípticas	
Nombre	**Descripción**
ECDSA (Elliptic Curve Digital Signature Algorithm)	Véase “algoritmos asimétricos de firma digital”
ECDH (Elliptic-curve Diffie-Hellman)	ECDH es una variante de DH (Diffie-Hellman) usando criptografía de curva elíptica. ECDH es un algoritmo de establecimiento de claves anónimo, el cual permite dos partes, cada una de las cuales tiene una llave del par de llaves (privada y pública) de curvas elípticas. Además, da la posibilidad de establecer un secreto compartido a través de un canal inseguro.

<table>
<tr><td></td><td>Este secreto compartido puede utilizarse tanto como llave como para derivar otra llave.
La llave o la llave derivada pueden utilizarse entonces para encriptar sucesivas comunicaciones utilizando un mismo cifrado de llave simétrica. Esta es una variante del protocolo.
Las curvas elípticas aprobadas para el acuerdo de llaves de ECQV son:

<table>
<tr><th>Curva</th><th>Fuerza de seguridad soportada</th></tr>
<tr><td>P-224</td><td>S = 112</td></tr>
<tr><td>P-256</td><td>112 ≤ s ≤ 128</td></tr>
<tr><td>P-384</td><td>112 ≤ s ≤ 192</td></tr>
<tr><td>P-521</td><td>112 ≤ s ≤ 256</td></tr>
<tr><td>K-233</td><td>112 ≤ s ≤ 128</td></tr>
<tr><td>K-283</td><td>112 ≤ s ≤ 128</td></tr>
<tr><td>K-409</td><td>112 ≤ s ≤ 192</td></tr>
<tr><td>K-571</td><td>112 ≤ s ≤ 256</td></tr>
<tr><td>B-233</td><td>112 ≤ s ≤128</td></tr>
<tr><td>B-283</td><td>112 ≤ s ≤ 128</td></tr>
<tr><td>B-409</td><td>112 ≤ s ≤ 192</td></tr>
<tr><td>B-571</td><td>112 ≤ s ≤ 256</td></tr>
</table>
</td></tr>
<tr><td>EdDSA (Edwards-curve Digital Signature Algorithm)</td><td>Véase “algoritmos asimétricos de firma digital”</td></tr>
<tr><td>ECMQV “Elliptic Curve Menezes-Qu-Vanstone” (Menezes–Qu–Vanstone con Curvas Elípticas)</td><td>Es un algoritmo variante de MQV, el cual usa criptografía de curvas elípticas a través de los esquemas que se basan también en curvas elípticas: Full MQV y One-Pass MQV.
Las curvas elípticas aprobadas para el acuerdo de llaves de ECQV son:</td></tr>
</table>

Curva	Fuerza de seguridad soportada
P-224	S = 112
P-256	$112 \leq s \leq 128$
P-384	$112 \leq s \leq 192$
P-521	$112 \leq s \leq 256$
K-233	$112 \leq s \leq 128$
K-283	$112 \leq s \leq 128$
K-409	$112 \leq s \leq 192$
K-571	$112 \leq s \leq 256$
B-233	$112 \leq s \leq 128$
B-283	$112 \leq s \leq 128$
B-409	$112 \leq s \leq 192$
B-571	$112 \leq s \leq 256$

Tabla 28: Algoritmos asimétricos de curvas elípticas

Fuente: FIPS PUB 186-4 y NIST Special Publication 800-56 A Revision 3

5.2.4 Algoritmos hash

Kaspersky (2022) define a estos tipos de algoritmos como: “Algoritmos matemáticos que transforman cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija” (s. p.).

5.2.4.1 Usos

Los algoritmos *hash* se usan para:

- Enmascaramiento de contraseñas, llaves y material clave.
- Detección de *malware* (firma de *malware*).
- Firma de material digital.
- Provee seguridad sobre la integridad de los datos y mensajes.

5.2.4.2 Detalles

Las características que comparten los buenos algoritmos *hash* son:

- **Determinismo**: Para una misma entrada (independientemente de su tamaño) siempre devolverá la misma salida de tamaño idéntico.
- **Resistencia previa a la imagen**: No es factible realizar el proceso inverso de un *hash* para recuperar el parámetro de entrada inicial.

- **Resistencia a la colisión**: Para cada parámetro de entrada siempre se obtiene una salida diferente, es decir, no se obtiene el mismo *hash* para dos entradas distintas.
- **Efecto avalancha**: Cualquier cambio al parámetro de entrada, sin importar el tamaño del cambio, siempre produce una salida totalmente distinta.
- **Velocidad del algoritmo *hash***: Se debe contar con una velocidad de procesamiento razonable que permita obtener los resultados en tiempos que no afecten la funcionalidad de las aplicaciones y sistemas.

5.2.4.3 Algoritmos hash aprobados

Hashes seguros	
Familia	Funciones
SHA-2	• SHA-224 • SHA-256 • SHA-384 • SHA-512 • SHA-512/224 • SHA-512/256 Ver las propiedades de estos algoritmos en Apéndice B y C.
SHA-3	• SHA3-224 • SHA3-256 • SHA3-384 • SHA3-512 Ver las propiedades de estos algoritmos en Apéndice C. **<u>Funciones de salida extensible</u>** • SHAKE128 • SHAKE256 • RawSHAKE128

	• RawSHAKE256 Estas funciones son equivalentes: SHAKE128 = RawSHAKE128 SHAKE256 = RawSHAKE256 Cada una de las funciones de salida extensible posee 128 *bits* y 256 *bits* correspondientes a la fuerza de seguridad proveída. **Funciones derivadas** • CSHAKE128 • CSHAKE256 • KMAC128 • KMAC256 • TupleHash128 • TupleHash256 • ParallelHash128 • ParallelHash256 Cada una de las funciones derivadas posee 128 bits y 256 bits correspondiente a la fuerza de seguridad proveída.

Tabla 29: Hashes seguros

Fuente: NIST SP 800-208, NIST SP 800-185.

5.3 Seleccionar la llave criptográfica

Con base en la publicación especial de NIST SP-800-57 Part 1 Revision 5-Recommendation for Key Management, existen muchos tipos diferentes de llaves criptográficas para diferentes propósitos, los cuales se clasifican en públicos, privados o simétricos (secretos) y sus diferentes usos. En cuanto a las llaves públicas y

privadas, su estado puede ser estático o efímero. La seguridad brindada por las llaves criptográficas depende específicamente de cuatro factores:

1) El algoritmo criptográfico en el que se usa.
2) La longitud de la llave.
3) El proceso que genera la llave.
4) El método de manejo de la llave (el transporte)

A continuación, se listan los diferentes tipos de llaves que existen según el enfoque dado:

5.3.1 Tipos de llaves criptográficas

Tipos de llaves	
Llave	Descripción
1. Llave de firma privada	Llave privada del par de llaves de los algoritmos de llave pública que se utiliza para generar firmas digitales para uso de largo plazo.
2. Llave de firma-verificación pública	Llave pública del par de llaves de los algoritmos de llave pública que se utiliza para verificar firmas digitales.
3. Llave de autenticación simétrica	Usada con los algoritmos de llaves simétricas para proveer autenticación de identidad y autenticación de integridad de sesiones de comunicación, mensajes, documentos o datos almacenados.
4. Llave de autenticación privada	Llave privada de los algoritmos de llave pública usada para proveer garantía de la identidad de una entidad cuando se establece una sesión de comunicación autenticada o acciones de autorización.
5. Llave de autenticación pública	Llave pública de los algoritmos de llave pública usada para proveer garantía de

	la identidad de una entidad cuando se establece una sesión de comunicación autenticada o acciones de autorización.
6. Llaves de encriptación de datos Simétrico	Usadas por los algoritmos de llave simétrica para aplicar protección de confidencialidad a los datos.
7. Llave de envoltura de llave simétrica	Además, conocidas como llaves de encriptación de llaves, las usan los algoritmos de llave simétrica para encriptar/desencriptar otras llaves.
8. Llaves RBG (generador de bits aleatorios) simétricas	Usadas para generar números o *bits* aleatorios.
9. Llave maestra simétrica/llave de derivación de llaves	Una llave maestra simétrica se usa para derivar otras llaves simétricas usando métodos de criptografía simétrica.
10. Llave de transporte de llave privada	Llave privada del par de llaves de los algoritmos de llaves públicas usadas para desencriptar llaves que se encriptan con la llave pública correspondiente usando un algoritmo de llave pública. Se utiliza para establecer llaves simétricas u otro material relacionado con la criptografía como los vectores de inicialización.
11. Llave de transporte de llave pública	Llave pública de los algoritmos de llaves públicas usadas para encriptar llaves usando un algoritmo de llave pública. Se usan para establecer llaves simétricas (llaves de envoltura de llaves, llaves para encriptación de datos o llaves MAC) u otro material criptográfico como los vectores de inicialización. Adicionalmente, puede almacenarse

	para desencriptar utilizando la llave de transporte de llave privada.
12. Llave de acuerdo de llave simétrica	Se usan para establecer llaves simétricas (llaves para envoltura de llave, llave para encriptación de datos o llaves MAC) y, opcionalmente, material criptográfico como los vectores de inicialización utilizando un algoritmo de acuerdo de llave simétrica.
13. Llave de acuerdo de llave estática privada	Es la llave privada de largo plazo de los algoritmos de llave pública usada para establecer llaves simétricas (llave para envoltura de llave, encriptación de datos o llave MAC) y, opcionalmente, material criptográfico como vectores de inicialización.
14. Llave de acuerdo de llave estática pública	Es la llave pública de largo plazo de los algoritmos de llave pública usados para establecer llaves simétricas (llave para envoltura de llave, encriptación de datos o llave MAC) y, opcionalmente, material criptográfico como vectores de inicialización.
15. Llave de acuerdo de llave efímera privada	Es la llave privada de corto plazo de los algoritmos de llave pública usados solo una vez para establecer una o más llaves simétricas (llave para envoltura de llave, encriptación de datos o llave MAC) y, opcionalmente, material criptográfico como vectores de inicialización.
16. Llave de acuerdo de llave efímera pública	Llave pública de corto plazo de los algoritmos de corto plazo usados en una única transacción de establecimiento de

	llave para establecer una o más llaves simétricas (llave para envoltura de llave, encriptación de datos o llave MAC) y, opcionalmente, material criptográfico como vectores de inicialización.
17. Llave de autorización simétrica	Se usan para proveer privilegios a una entidad por medio de criptografía simétrica. La llave es conocida tanto por la organización que brinda la autorización de acceso como por la entidad que busca el acceso a los recursos.
18. Llave de autorización privada	Es la llave privada de los algoritmos de llave pública usada para proveer los derechos a los privilegios del usuario (usando firma digital).
19. Llave de autorización pública	Llave pública de los algoritmos de llave pública usada para verificar los privilegios de una entidad que conoce la llave de autorización privada asociada.

Tabla 30: Tipos de llaves

Fuente: NIST Special Publication 800-57 Part 1 Revision 5.

5.3.2 Protección de las llaves criptográficas

Requerimientos para la protección de llaves criptográficas					
Tipo de llave	**Servicio de seguridad**	**Protección de seguridad**	**Protección de la asociación**	**Garantía requerida**	**Periodo de protección**
1. Llave de firma privada	Fuente de autenticación Autenticación de integridad	Confidencialidad Integridad	Uso o aplicación Parámetros de dominio	Posesión	Desde la generación hasta el fin del criptoperiodo

	Soporte para no repudio		(cuando se usan) Llave de firma o verificación pública		
2. Llave de firma-verificación pública	Fuente de autenticación Autenticación de integridad Soporte para no repudio	Integridad Disponibilidad	Uso o aplicación Propietario del par de llaves Parámetros de dominio (cuando se usan) Llave privada Datos firmados	Validez	Desde la generación hasta que ningún dato protegido necesite verificarse
3. Llave de autenticación simétrica	Autenticación de identidad Autenticación de integridad	Confidencialidad Integridad Disponibilidad	Uso o aplicación Otras entidades autorizadas Datos autenticados		Desde la generación hasta que ningún dato protegido necesite verificarse
4. Llave de autenticación privada	Autenticación de identidad Autenticación de integridad	Confidencialidad Integridad	Uso o aplicación Llave de autenticación pública	Posesión	Desde la generación hasta el fin del criptoperiodo

			Parámetros de dominio (cuando se usan)		
5. Llave de autenticación pública	Autenticación de identidad Autenticación de integridad	Integridad Disponibilidad	Uso o aplicación Propietario del par de llaves Datos autenticados Llave de autenticación privada Parámetros de dominio (cuando se usan)	Validez	Desde la generación hasta que ningún dato protegido necesite autenticarse
6. Llaves de encriptación de datos simétricos	Confidencialidad	Confidencialidad Integridad Disponibilidad	Uso o aplicación Otras entidades autorizadas Datos encriptados/texto plano		Desde la generación hasta el fin de la vida de los datos o el fin del criptoperiodo, lo que ocurra más tarde
7. Llave de envoltura de llave simétrica	Soporte	Confidencialidad Integridad Disponibilidad	Uso o aplicación Otras entidades autorizadas		Desde la generación hasta el fin del criptoperiodo o hasta que

			Llaves encriptadas		ninguna llave de envoltura requiera protección, lo que ocurra más tarde
8. Llaves RBG (generador de *bits* aleatorios) simétricas	Soporte	Confidencialidad Integridad	Uso o aplicación		Desde la generación hasta el reemplazo
9. Llave maestra simétrica/llave de derivación de llaves	Soporte	Confidencialidad Integridad	Uso o aplicación Otras entidades autorizadas Llaves derivadas		Desde la generación hasta el fin del criptoperiodo o el fin de la vida de las llaves derivadas, lo que ocurra más tarde
10. Llave de transporte de llave privada	Soporte	Confidencialidad Integridad Disponibilidad	Uso o aplicación Llaves encriptadas Llave pública de transporte de llaves	Posesión	Desde la generación hasta el fin del periodo de protección para todas las llaves transportadas
11. Llave de transporte de llave pública	Soporte	Integridad	Uso o aplicación	Validez	Desde la generación hasta el fin del

			Propietario del par de llaves Llave privada de transporte de llaves		criptoperiodo
12. Llave de acuerdo de llave simétrica	Soporte	Confidencialidad Integridad	Uso o aplicación Otras entidades autorizadas		Desde la generación hasta el fin del criptoperiodo o hasta que no se necesite determinar una llave, lo que ocurra más tarde
13. Llave de acuerdo de llave estática privada	Soporte	Confidencialidad Integridad	Uso o aplicación Parámetros de dominio (cuando se usan) Llave pública estática de acuerdo de llaves	Posesión	Desde la generación hasta el fin del criptoperiodo o hasta que ya no se necesite determinar una llave, lo que ocurra más tarde
14. Llave de acuerdo de llave estática pública	Soporte	Integridad	Uso o aplicación Parámetros de dominio (cuando se usan)	Validez	Desde la generación hasta el fin del criptoperiodo o hasta que ya no se necesite

			Llave privada estática de acuerdo de llaves		determinar una llave, lo que ocurra más tarde
15. Llave de acuerdo de llave efímera privada	Soporte	Confidencialidad Integridad	Uso o aplicación Llave pública efímera de acuerdo de llaves		Desde la generación hasta el fin del proceso de acuerdo de llave. Después del fin del proceso, la llave debe ser destruida
16. Llave de acuerdo de llave efímera pública	Soporte	Integridad	Uso o aplicación Parámetros de dominio (cuando se usan) Llave privada efímera de acuerdo de llaves	Validez	Desde la generación hasta que el proceso de acuerdo de llaves sea completado
17. Llave de autorización simétrica	Autorización	Confidencialidad Integridad	Uso o aplicación Otras entidades autorizadas		Desde la generación hasta el fin del criptoperiodo de la llave
18. Llave de autorización privada	Autorización	Confidencialidad Integridad	Uso o aplicación	Posesión	Desde la generación hasta el fin del

			Llave pública de autorización Parámetros de dominio (cuando se usan)		criptoperiodo de la llave
19. Llave de autorización pública	Autorización	Integridad	Uso o aplicación Llave privada de autorización Parámetros de dominio (cuando se usan)	Validez	Desde la generación hasta el fin del criptoperiodo de la llave

Tabla 31: Requerimientos para la protección de llaves criptográficas

Fuente: NIST Special Publication 800-57 Part 1 Revision 5.

5.3.3 Plazo de protección de las llaves criptográficas

Plazos de las fuerzas de seguridad de las llaves			
Fuerza de seguridad (bits)		**Hasta el año 2030**	**Después del año 2031**
<112	Aplicando protección	Deshabilitado	
	Procesamiento	Uso heredado	
112	Aplicando protección	Aceptable	Deshabilitado
	Procesamiento		Uso heredado
128	Aplicar la protección y el procesamiento de información que ya está protegida	Aceptable	Aceptable
192		Aceptable	Aceptable
256		Aceptable	Aceptable

Tabla 32: Plazos de las fuerzas de seguridad de las llaves

Fuente: NIST Special Publication 800-57 Part 1 Revision 5.

5.3.4 Comparación de eficacia para las llaves criptográficas

Comparación de eficacia de la fuerza de la seguridad proveída por los algoritmos simétricos de cifrado por bloque y algoritmos asimétricos.				
Fuerza de seguridad	**Algoritmos de llave simétrica**	**FFC (DSA, DH, MQV)**	**IFC* (RSA)**	**ECC* (ECDSA, EdDSA, DH, MQV)**
112	3TDEA	*L* = 2048 *N* = 224	*K* = 2048	*F* = 224-255
128	AES-128	*L* = 3072 *N* = 256	*K* = 3072	*F* = 256-383
192	AES-192	*L* = 7680 *N* = 384	*K* = 7680	*F* = 384-511
256	AES-256	*L* = 15360 *N* = 512	*K* = 15360	*F* = 512+

Tabla 33: Comparación de eficacia de la fuerza de la seguridad proveída por los algoritmos simétricos de cifrado por bloque y algoritmos asimétricos
Fuente: NIST Special Publication 800-57 Part 1 Revision 5.

Columna 1: Indica el nivel de seguridad máximo estimado (en *bits*) que proporcionan los algoritmos y las longitudes de clave que aparecen en una fila determinada. Obsérvese que el nivel de seguridad no es necesariamente el mismo que la longitud de la clave, debido a los ataques a los algoritmos que proporcionan ventajas computacionales.

Columna 2: Identifica los algoritmos de clave simétrica que pueden proporcionar la fuerza de seguridad indicada en la columna 1, donde 3TDEA se especifica en SP800-67 y AES se especifica en FIPS 197. 2TDEA es TDEA con dos claves diferentes; 3TDEA es TDEA con tres claves distinta. Se debe tener en cuenta que se han aprobado modos de operación y RBG que utilizan estos cifrados de bloque como primitivas criptográficas (ver serie SP 800-38 y SP 800-90 A). Los puntos fuertes de seguridad

proporcionados por estos algoritmos son los mismos que los proporcionados por sus primitivas.

Columna 3: Indica el tamaño mínimo de los parámetros asociados con las normas que utilizan la criptografía de campo finito (FFC). Algunos ejemplos de estos algoritmos son DSA, como se define en el FIPS 186 para las firmas digitales y el acuerdo de claves Diffie-Hellman (DH) y MQV, como se definen en el SP 800-56 A, donde L es el tamaño de la clave pública y N es el tamaño de la clave privada.

Columna 4: Indica el valor de k (el tamaño del módulo n) para los algoritmos con base en criptografía de factorización entera (IFC). El algoritmo predominante de este tipo es el algoritmo RSA. El RSA está aprobado en el FIPS 186 para las firmas digitales y en el SP 800-56B para establecer claves. El valor de k se considera comúnmente como el tamaño de la clave.

Columna 5: Indica el rango de f (el tamaño de n, donde n es el orden del punto base G) para los algoritmos con base en la criptografía de curva elíptica (ECC) que se especifican para las firmas en FIPS 186 y para establecer claves según se especifica en SP 800-56 A. El valor de f se considera comúnmente como el tamaño de la clave.

5.3.5 Comparación de eficacia para hashes.

Máximos niveles de seguridad para las funciones hash y con base en hash		
Fuerza de seguridad	Firma digital y otras aplicaciones que requieren resistencia a colisiones	HMAC, KMAC, Funciones de derivación de llave, generación de *bits* aleatorios
112	SHA-224 SHA-512/224 SHA3-224	-
128	SHA-256 SHA-512/256 SHA3-256	SHA-1 KMAC128
192	SHA-384 SHA3-384	SHA-224 SHA-512/224 SHA3-224
≥ 256	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-256 SHA3-384 SHA3-512 KMAC256

Tabla 34: Máximos niveles de seguridad para las funciones hash y con base en hash

Fuente: NIST Special Publication 800-57 Part 1 Revision 5.

5.3.6 Estados de las llaves criptográficas.

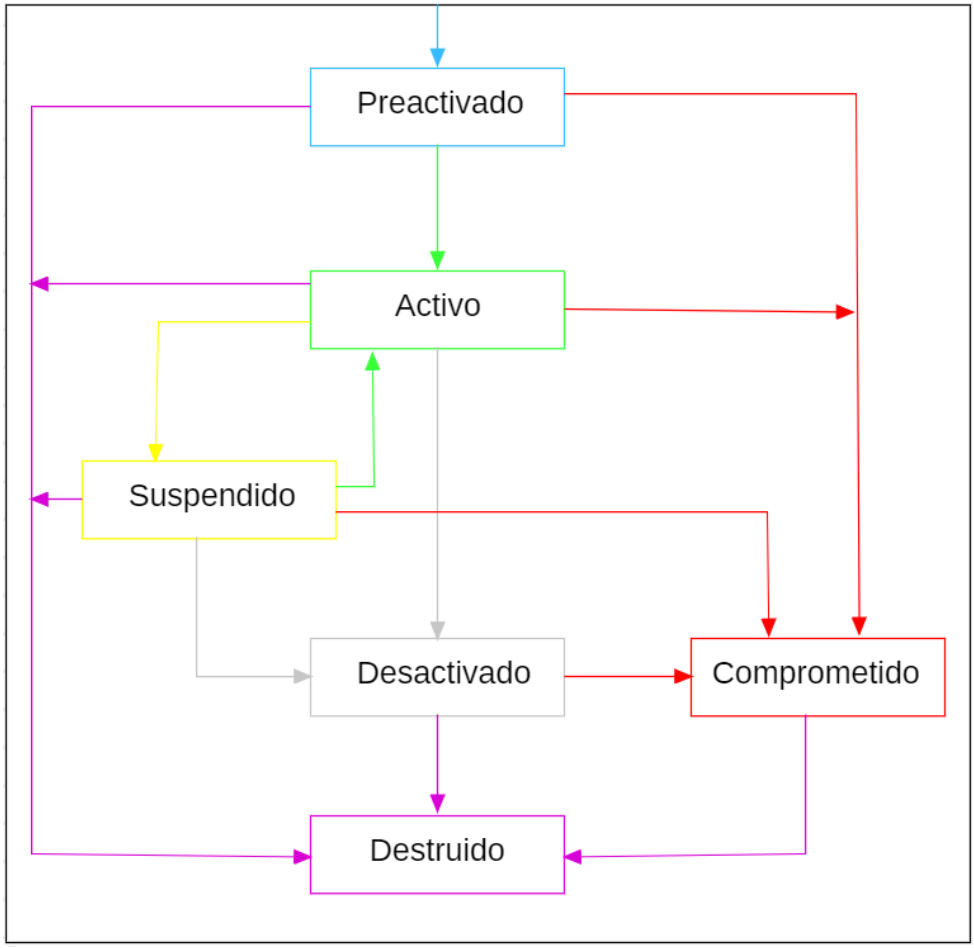

Figura 32: Estados de las llaves criptográficas

Basado: NIST Special Publication 800-57 Part 1 Revision 5

5.4 Seleccionar los datos relacionados con la criptografía

Aparte de los algoritmos y llaves criptográficas, otra información criptográfica que también se debe proteger es la siguiente:

Otra información criptográfica	
Parámetros de dominio	Usados por algoritmos de llave pública para generar el par de llaves, crear firmas digitales o establecer material clave.
Vectores de inicialización	También conocidos simplemente como VI, los usan muchos modos de

	operación para encriptar/desencriptar y para computar las MAC usando algoritmos de cifrado por bloques.
Secretos compartidos	Se generan durante el proceso de acuerdo de llaves.
Semillas de RBG (generador de bits aleatorios)	Usadas en la generación de *bits* aleatorios determinísticos (materia clave que debe permanecer secreta o privada).
Otra información pública	Se usan en el proceso de establecimiento de llaves (por ej. *nonce*).
Otra información secreta	Puede ser incluida en la semilla para un RGB o en el establecimiento de material clave.
Resultados intermedios	Estos son los resultados intermedios en las operaciones criptográficas.
Información/metadatos de control de claves	Información relacionada con el material clave (identificadores, propósitos o contadores) que debe protegerse para asegurar que el material clave pueda usarse correctamente.
Números/bits aleatorios	Números aleatorios creados por un RGB.
Contraseña	Usado para adquirir acceso a privilegios, además de poderse utilizar como credenciales en mecanismos de autenticación de recursos o autenticación de identidad.

Tabla 35: Otra información criptográfica

Fuente: NIST Special Publication 800-57 Part 1 Revision 5

Requerimientos de protección para otros datos que se relacionan con la llave criptográfica					
Tipo de información	**Servicio de seguridad**	**Protección de seguridad**	**Protección de la asociación**	**Garantía de la validez de los parámetros de dominio**	**Periodo de protección**
Parámetros de dominio	Depende de la llave asociada con los parámetros	Integridad Disponibilidad	Uso o aplicación Llaves privadas y públicas	Sí	Desde la generación hasta que se necesite para generar llaves o verificar firmas
Vectores de inicialización	Depende del algoritmo	Integridad Disponibilidad	Datos protegidos		Desde la generación
Secretos compartidos	Soporte	Integridad Confidencialidad			Desde la generación hasta el final de la transacción Deberá ser destruido al final del periodo de protección

Semillas RBG	Soporte	Integridad Confidencialidad	Uso o aplicación		Usadas una única vez y destruidas inmediatamente después de su uso
Otras informaciones públicas	Soporte	Integridad	Uso o aplicación Otras entidades autorizadas Datos procesados usando un *nonce*		Desde la generación hasta que no se necesite para procesar datos usando información pública
Otras informaciones secretas	Soporte	Integridad Confidencialidad	Uso o aplicación Otras entidades autorizadas Datos procesados usando		Desde la generación hasta que no se necesite para procesar datos usando información secreta

			información secreta		
Resultados intermedios	Soporte	Integridad Confidencialidad	Uso o aplicación		Desde la generación hasta que no se necesite y, posteriormente, debe ser destruida
Información de control de llaves	Soporte	Integridad Disponibilidad	Llave		Desde la generación hasta que la llave asociada se destruya
Números aleatorios	Soporte	Integridad Confidencialidad (depende del uso)			Desde la generación hasta que no se necesite. Después el número aleatorio debe ser destruido
Contraseña	Autenticación de identidad Derivación de llaves	Integridad Confidencialidad Disponibilidad	Uso o aplicación Entidad del propietario		Desde la generación hasta el reemplazo o que necesite para autenticar la

					entidad o derivar llave
Información de auditoría	Soporte	Integridad Autorización de acceso Disponibilidad	Eventos auditados Metadatos o información de control de llave		Desde la generación hasta que no se necesite

Tabla 36: Requerimientos de protección para otros datos que se relacionan con la llave criptográfica

Fuente: NIST Special Publication 800-57 Part 1 Revision 5.

5.4.1 Metadatos

- Identificador de la llave.
- Algoritmo usado con la llave.
- Información al identificar las llaves asociadas (por ej., la asociación entre las llaves privadas y públicas).
- Identidad del propietario de la llave o las entidades que comparten.
- Identidad de los patrocinadores o representantes para el propietario (si el propietario no es una entidad humana).
- Indicación sobre si el propietario es un dispositivo o un proceso, además de su localización.
- El cripto periodo de la llave (por ej., fechas de inicio y fin para el uso de la llave).
- Tipo de llave (por ej., llave privada para firmar, llave para encriptación o llave maestra).
- Fuente del material de encriptación (por ej., la entidad que provee la llave).
- Aplicación o uso de la llave (por ej., compras o correos electrónicos).
- Sensibilidad de la información siendo protegida por la llave.

- Un contador.
- Estado actual de la llave (por ej., preactivación, activo, destruido).
- Historial de los estados de la llave (por ej., distribuida, suspendida, revocada).
- Identidad de la llave que envuelve otras llaves y el algoritmo usado para su proceso.
- Mecanismo para la protección de integridad usado.
- Otra información (por ej., longitud de la llave, requerimientos de protección, quién tiene derecho de acceso a la llave, condiciones adicionales para su uso).

5.4.2 Técnicas de cifrado

Técnicas de cifrado en bloque	
Modos de confidencialidad	
Modo	**Descripción**
ECB "Electronic CodeBook" (libro de códigos electrónico)	Es un modo de confidencialidad que se presenta para una clave determinada la asignación de un bloque de texto cifrado fijo a cada bloque de texto plano, de forma análoga a la asignación de palabras clave en un libro de códigos. La función de cifrado hacia adelante se aplica directa e independientemente a cada bloque del texto plano. La secuencia resultante de bloques de salida es el texto cifrado. La función de cifrada inversa se aplica directa e independientemente a cada bloque del texto cifrado. La secuencia resultante de bloques de salida es el texto plano.
CBC "Cipher Block Chaining" (encadenamiento de bloques de cifrado)	Es un modo de confidencialidad cuyo proceso de cifrado consiste en combinar (*encadenar*) los bloques de texto plano

	con los bloques de texto cifrado anteriores. El modo CBC requiere un VI (vector de inicialización) para combinar con el primer bloque de texto plano. El VI no tiene por qué ser secreto, pero debe ser imprevisible.
CFB "Cipher Feed Back" (retroalimentación del cifrado)	Es un modo de confidencialidad que presenta la retroalimentación de segmentos sucesivos de texto cifrado en los bloques de entrada del cifrado hacia adelante para generar bloques de salida que se unen de forma exclusiva con el texto plano para producir el texto cifrado y viceversa. El modo CFB requiere un VI (vector de inicialización) para combinar con el primer bloque de texto plano. El VI no tiene por qué ser secreto, pero debe ser imprevisible.
OFB "Output Feed Back" (retroalimentación de salida)	Es un modo de confidencialidad que presenta la iteración de un VI (vector de inicialización) para generar una secuencia de bloques de salida que se unen con el texto plano para producir el texto cifrado y viceversa. El modo OFB requiere que el VI sea un *nonce*, es decir, el VI debe ser único para cada ejecución del modo bajo la clave dada.
CTR "Counter Mode" (modo contador)	Es un modo de confidencialidad que consiste en aplicar el cifrado hacia delante a un conjunto de bloques de

	entrada, llamados contadores, para producir una secuencia de bloques de salida que se unen de forma exclusiva con el texto plano para producir el texto cifrado y viceversa. La secuencia de contadores debe tener la propiedad de que cada bloque de la secuencia es diferente de cualquier otro bloque. Esta condición no se limita a un solo mensaje: en todos los mensajes que se cifren con la clave dada todos los contadores deben ser distintos. En esta recomendación, los contadores de un mensaje determinado se denominan T_1, T_2..., T_n
Modo de autenticación	
Modo	**Descripción**
CMAC "Cipher-based Message Authentication Code (MAC)" (código de autenticación de mensajes [MAC] con base en el cifrado)	Depende de la elección de un cifrado de bloques de clave simétrica subyacente. El algoritmo CMAC es, por lo tanto, un modo de funcionamiento (un modo para abreviar) del cifrado por bloques. La clave CMAC es la clave del cifrado por bloques (la clave para abreviar). Para cualquier clave dada, el cifrado por bloques subyacente del modo consiste en dos funciones que son inversas entre sí. La elección del cifrado por bloques incluye la designación de una de las dos funciones del cifrado por bloques como

	la función/transformación directa y la otra como la función inversa función. La función de cifrado hacia adelante es una permutación en cadenas de *bits* de una longitud fija; las cadenas se llaman bloques. La longitud de los *bits* de un bloque se denomina b y la longitud de un bloque se llama tamaño del bloque.
Modo de cifrado autenticado	
Modo	**Descripción**
CCM "Counter with Cipher Block Chaining-Message Authentication Code" (contador con código de encadenamiento de bloques de cifrado-mensaje de autenticación)	Depende de la elección de un algoritmo de cifrado por bloques de clave simétrica subyacente. El algoritmo CCM es, por lo tanto, un modo de operación del cifrado por bloques de clave simétrica por bloques. El algoritmo de cifrado por bloques subyacente debe aprobarse y una clave secreta para el algoritmo de cifrado por bloques se genera uniformemente al azar o casi uniformemente al azar, es decir, de manera que cada clave posible tenga (casi) la misma probabilidad de generarse. Además, la clave debe establecerse para las partes de la información mediante un método aprobado de establecimiento de claves. La clave se mantiene en secreto y solo se utiliza para el modo MCP. El número total de invocaciones del algoritmo de

	cifrado por bloques durante el tiempo de vida de la clave está limitado a 261.
Modo de cifrado autentificado de alto rendimiento	
Modo	**Descripción**
GCM "Galois/Counter Mode" (modo Galois/Counter)	Las operaciones de GCM dependen de la elección de un cifrado por bloques de clave simétrica subyacente, por lo que puede considerarse un modo de operación del cifrado por bloques. Para cualquier clave dada, el cifrado por bloques subyacente del modo consiste en dos funciones que son inversas entre sí. La elección del cifrado por bloques incluye la designación de una de las dos funciones del cifrado por bloques como la función de cifrado hacia adelante. Esta es una permutación sobre cadenas de *bits* de una longitud fija; las cadenas se denominan bloques. La longitud de un bloque se denomina tamaño de bloque. La clave se denomina K y la función de cifrado hacia adelante resultante del cifrado por bloques se denomina $CIPH_k$.
Modo de confidencialidad diseñado para los dispositivos de almacenamiento	
Modo	**Descripción**
XTS-AES "XEX Tweakable Block Cipher with Ciphertext Stealing" (cifrado en bloque modificable XEX con texto cifrado de robo)	El algoritmo XTS-AES es un modo de funcionamiento del estándar de cifrado avanzado (AES). El modo XTS-AES se diseñó para la protección criptográfica de datos en dispositivos de almacenamiento que

	utilizan unidades de datos de longitud fija. Se debe tener en cuenta que otros algoritmos criptográficos son aprobados para tales dispositivos. El modo XTS-AES no se diseñó para otros fines, como el cifrado de datos en tránsito.
Métodos de envoltura de llaves	
Modo	**Descripción**
KW "AES Key Wrap" (envoltura de llave AES)	Modo de funcionamiento de cifrado autenticado determinista del cifrado en bloque del estándar de cifrado avanzado (AES). Puede utilizarse junto con cualquier reversible, también se especifica una variante de KW con un esquema de relleno interno para promover la interoperabilidad (KWP).
KWP "AES Key Wrap with Padding" (envoltura de llave AES con relleno)	Variante del modo KW.
Métodos de cifrado con preservación del formato	
Modo	**Descripción**
FF1 "Feistel-based Format-preserving encryption o FF" (encriptación que preserva el formato que se basa en Feistel)	Emplea la estructura de Feistel. FF1 admite una mayor gama para los datos protegidos y formateados, así como una mayor flexibilidad en la longitud del ajuste.
FF3-1 "Feistel-based Format-preserving encryption o FF" (encriptación que preserva el formato que se basa en Feistel)	Emplea la estructura de Feistel. FF3-1 consigue un mayor rendimiento, principalmente porque tiene ocho rondas, frente a las diez del FF1.

Tabla 37: Técnicas de cifrado en bloque

Fuente: NIST Special Publication 800-38 A 2001 Edition.

NIST Special Publication 800-38B.

NIST Special Publication 800-38C.

NIST Special Publication 800-38D November (2007).

NIST Special Publication 800-38E January (2010).

NIST Special Publication 800-38F December (2012).

NIST Special Publication 800-38G.

5.5 Definir el criptoperiodo

Los siguientes periodos para cada tipo de llave son los que recomienda NIST en su publicación especial “NIST Special Publication 800-57 Part 1 Revision 5”.

Tipo de llave	**Criptoperiodos**	
	Periodo de uso del creador (PUC)	Periodo de uso del destinatario
1. Llave de firma privada	1 a 3 años	-
2. Llave de firma-verificación pública	Muchos años (según tamaño de la llave)	
3. Llave de autenticación simétrica	≤ 2 años	≤ PUC + 3 años
4. Llave de autenticación privada	1 a 2 años	
5. Llave de autenticación pública	1 a 2 años	
6. Llaves de encriptación de datos simétrica	≤ 2 años	≤ PUC + 3 años
7. Llave de envoltura de llave simétrica	≤ 2 años	≤ PUC + 3 años
8. Llaves RBG (generador de *bits* aleatorios) simétricas	Ver SP 800-90	-
9. Llave maestra simétrica/llave de derivación de llaves	Alrededor de 1 año	-
10. Llave de transporte de llave privada	≤ 2 años	
11. Llave de transporte de llave pública	1 a 2 años	

12. Llave de acuerdo de llave simétrica	1 a 2 años
13. Llave de acuerdo de llave estática privada	1 a 2 años
14. Llave de acuerdo de llave estática pública	1 a 2 años
15. Llave de acuerdo de llave efímera privada	Una transacción de acuerdo llave
16. Llave de acuerdo de llave efímera pública	Una transacción de acuerdo llave
17. Llave de autorización simétrica	≤ 2 años
18. Llave de autorización privada	≤ 2 años
19. Llave de autorización pública	≤ 2 años

Tabla 38: Criptoperiodos

Fuente: NIST Special Publication 800-57 Part 1 Revision 5.

Verificar que no existan los siguientes factores que afectan los criptoperiodos.

- La fuerza de los mecanismos criptográficos (por ej., algoritmo, longitud de llave, tamaño de bloque y modo de operación).
- La realización (implementación) de los mecanismos.
- El ambiente operativo (por ej., una instalación segura de acceso limitado, ambiente de oficina abierto o terminal públicamente accesible).
- Rotación del personal (por ej., administradores de sistemas, personal de sistemas CA “autoridad certificadora”).
- El volumen del flujo de datos o el número de transacciones.
- La vida de seguridad de los datos.
- Limitaciones requeridas para el uso de los algoritmos (por ej., número máximo de invocaciones para evitar el continuo uso del *nonce*).
- Las funciones de seguridad (por ej., encriptación de datos, firma digital, derivación de llave o protección de la llave).

- El método de reentrada de datos (por ej., teclado, dispositivo de carga de llave donde las personas no tienen acceso directo a las llaves o reentrada utilizando PKI).
- El proceso usado para la derivación y reentrada de la llave.
- El número de nodos en la red donde se comparte la llave.
- El número de copias de la llave y la distribución de sus copias.
- Las amenazas de la información por los adversarios (por ej., habilidades técnicas y recursos financieros al ataque).
- La amenaza a la información por nuevas y disruptivas tecnologías (por ej., computadoras cuánticas).

5.6 Generar y distribuir las llaves criptográficas

Las llaves simétricas y asimétricas deben crearse a través de los RBG (generador de *bits* aleatorios) aprobados (SP 800-90 A Revision 1). Los generadores de *bits* aleatorios utilizan mecanismos que usan la entropía para brindar un resultado aleatorio en forma de cadena de *bits*, los cuales se utilizan como la llave criptográfica, como lo define y detalla NIST en SP 800-90 A Revision: “Un dispositivo o algoritmo que produce una secuencia de bits binarios que parece ser estadísticamente independiente e imparcial” (s. p.).

Generadores de *bits* aleatorio (RBG)	
Mecanismos	**Funciones**
Con base en funciones *hash*	Hash_DRBG
	HMAC_DRBG
Con base en cifrado por bloques	CTR_DRBG
Funciones auxiliares	Hash_df (Función de derivación usando una función hash)
	Block_Cipher_df (Función de derivación usando un algoritmo de cifrado por bloques)

Tabla 39: Generadores de bits aleatorio (RBG)

Fuente: NIST Special Publication 800-90 A Revision 1.

5.6.1 Llaves simétricas

Una vez que se han estudiado los requerimientos y se hayan decantado las llaves simétricas lo siguiente es la generación y distribución para iniciar con su uso. La clave secreta es generada por:

- Una o varias de las entidades que compartirán la clave.
- Un tercero de confianza que proporcione la clave a las entidades que pretenden compartirla de forma segura. Todas las entidades que compartan la clave deben confiar en el tercero de confianza para que no revele la clave a terceros no autorizados o hacer un mal uso de esta (ver SP 800-71).

Se puede utilizar una clave simétrica, por ejemplo, para:

- Encriptar y desencriptar datos en un modo apropiado (ver FIPS 197 y SP 800-38 A)
- Generar código de autenticación de mensajes (AES con modo CMAC en FIPS 197 y “SP 800-38B” o HMAC en FIPS 198 o KMAC en “SP 800-185”)
- Derivar llaves adicionales utilizando una función de derivación de llaves especificada en el SP 800-108, donde K es la clave precompartida (es decir, preexistente) que se utiliza como clave de derivación de llave.

5.6.1 Generación

A continuación, se detallan los métodos aprobados actualmente, los cuales se basan directa o indirectamente sobre el resultado de un RBG: (ver: SP 800-133 Revision 2):

1) La generación directa de llaves simétricas

   La llave simétrica es el resultado obtenido directamente de la salida de un RBG.

   Se debe validar la longitud de la llave según los requerimientos y el algoritmo criptográfico aprobado con el cual se utiliza la llave.

   NIST en su SP 800-90C.3 explica en detalle las bondades de los RBG y su implementación según la necesidad presentada.

2) Derivación de llaves simétricas

Una derivación de llaves es el resultado de un método de derivación de llaves (KDM *key-derivation method*) aprobado que consiste en el proceso criptográfico en donde se transforman los parámetros secretos de entrada a cadenas de bits. Estos pueden utilizarse como llaves criptográficas o como parámetros secretos de entrada para otro proceso utilizando KDM.

Según la aplicación y el KDM que se utiliza puede incluir como parámetros lo siguiente:

- ✓ Un valor de secreto compartido producido durante la ejecución de un esquema de acuerdo de llaves.
- ✓ Una llave criptográfica (ejemplo: una llave derivada).
- ✓ Una contraseña o frase de acceso.
- ✓ Un valor *salt*
- ✓ Un *nonce*

Los KDM aprobados (ver SP.800-56Cr2) son los siguientes:

- Derivación de llaves en un solo paso
  - ➢ Con base en HASH: Función -> hash(x)

Función hash	Longitud en byte/bit de bloques de entrada	Bits de salida	Longitud de entrada máxima (en bits)	Fuerza de seguridad s soportada (en bits)
SHA-1	64/512	160	$\leq 2^{64}-1$	112 ≤ s ≤ 160
SHA-224	64/512	224		112 ≤ s ≤ 224
SHA-256	64/512	256		112 ≤ s ≤ 256
SHA-512/224	128/1024	224	$\leq 2^{128}-1$	112 ≤ s ≤ 224
SHA-512/256	128/1024	256		112 ≤ s ≤ 256
SHA-384	128/1024	384		112 ≤ s ≤ 384
SHA-512	128/1024	512		112 ≤ s ≤ 512
SHA3-224	114/1152	224	Entradas con longitudes arbitrarias	112 ≤ s ≤ 224
SHA3-256	136/1088	256		112 ≤ s ≤ 256
SHA3-384	104/832	384		112 ≤ s ≤ 384

SHA3-512	72/576	512	pueden ser acomodadas	112 ≤ s ≤ 512

Tabla 40: Derivación de llaves con base en funciones hash

Fuente: NIST Special Publication 800-56C Revision 2.

- Con base en HMAC: Función -> HMAC-hash(salt, x)

Función hash	Longitud efectiva en byte/bit del salt	Bits de salida	Longitud de entrada máxima (en bits)	Fuerza de seguridad s soportada (en bits)
SHA-1	64/512	160	≤ 2^{65}-513	112 ≤ s ≤ 160
SHA-224	64/512	224		112 ≤ s ≤ 224
SHA-256	64/512	256		112 ≤ s ≤ 256
SHA-512/224	128/1024	224	≤ 2^{128} - 1025	112 ≤ s ≤ 224
SHA-512/256	128/1024	256		112 ≤ s ≤ 256
SHA-384	128/1024	384		112 ≤ s ≤ 384
SHA-512	128/1024	512		112 ≤ s ≤ 512
SHA3-224	144/1152	224	Entradas con longitudes arbitrarias pueden ser acomodadas	112 ≤ s ≤ 224
SHA3-256	136/1088	256		112 ≤ s ≤ 256
SHA3-384	104/832	384		112 ≤ s ≤ 384
SHA3-512	72/576	512		112 ≤ s ≤ 512

Tabla 41: Derivación de llaves con base en funciones HMAC

Fuente: NIST Special Publication 800-56C Revision 2.

- Con base en KMAC: Función -> KMAC#(salt, x, bits de salida, “KDF”)

Donde KDF = Función de derivación de llave

Variante KMAC	Longitud del valor codificado del salt	Longitud máxima sugerido de bytes de la sal	Bits de salida	Longitud de entrada máxima (en bits)	Fuerza de seguridad s soportada (en bits)
KMAC128	Múltiplo de 168 *bytes*	168 – 4 = 164	Selección de: • 160 • 224 • 256 • 384 • 512 • Un número entero positivo que especifica la longitud deseada	Entradas con longitudes arbitrarias pueden ser acomodadas	112 ≤ s ≤ 128
KMAC256	Múltiplo de 136 *bytes*	136 – 4 = 132			112 ≤ s ≤ 256

Tabla 42: Derivación de llaves con base en funciones KMAC

Fuente: NIST Special Publication 800-56C Revision 2.

- Derivación de llaves en dos pasos

  Consiste en el procedimiento de extraer y después expandir la llave derivada, lo cual envuelve dos pasos. A continuación, se muestra el mecanismo que se utiliza para derivar llaves en dos pasos:

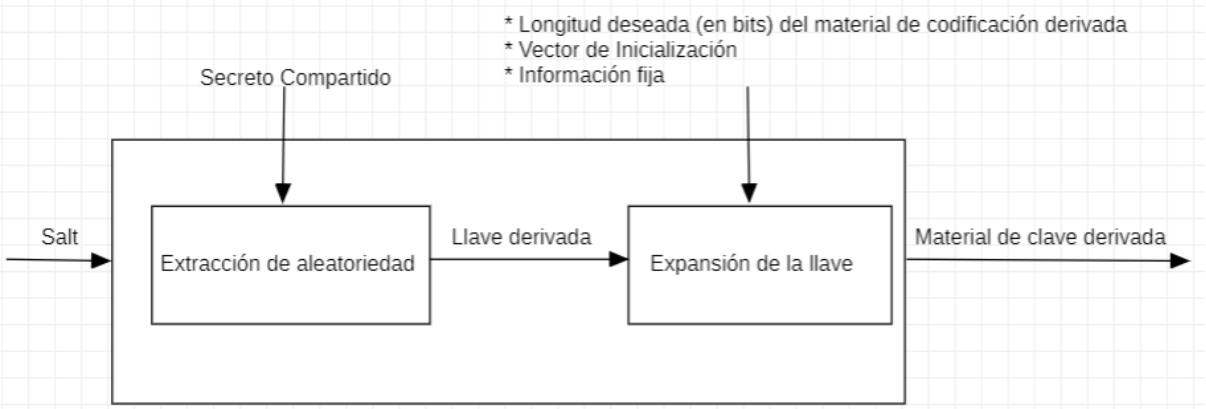

Figura 33: Proceso de la derivación de llaves en dos pasos

Fuente: NIST Special Publication 800-56C Revision 2.

- Extracción de aleatoriedad

Obtiene una única llave criptográfica de derivación.

Función hash	Longitud efectiva en byte/bit del salt	Longitud de bit de la llave derivada	Fuerza de seguridad s soportada (en bits)
SHA-1	64/512	160	112 ≤ s ≤ 160
SHA-224	64/512	224	112 ≤ s ≤ 224
SHA-256	64/512	256	112 ≤ s ≤ 256
SHA-512/224	128/1024	224	112 ≤ s ≤ 224
SHA-512/256	128/1024	256	112 ≤ s ≤ 256
SHA-384	128/1024	384	112 ≤ s ≤ 384
SHA-512	128/1024	512	112 ≤ s ≤ 512
SHA3-224	144/1152	224	112 ≤ s ≤ 224
SHA3-256	136/1088	256	112 ≤ s ≤ 256
SHA3-384	104/832	384	112 ≤ s ≤ 384
SHA3-512	72/576	512	112 ≤ s ≤ 512

Tabla 43: Algoritmos MAC = HMAC para extracción de aleatoriedad

Fuente: NIST Special Publication 800-56C Revision 2.

Variante AES usado por AES-CMAC	Longitud de bits del salt para AES-CMAC	Longitud de bit de la llave derivada	Fuerza de seguridad s soportada (en bits)
AES-128	128	128	112 ≤ s ≤ 128
AES-192	192		
AES-256	256		

Tabla 44: Algoritmos MAC = AES-N-CMAC para extracción de aleatoriedad

Fuente: NIST Special Publication 800-56C Revision 2.

- Expansión de la llave

  Deriva el material clave desde:

  - La llave derivada producida durante la extracción de aleatoriedad.
  - Otra información.

  Diferentes *secretos compartidos* y *salt* producirán distintas llaves derivadas y estas se utilizan en el proceso de expansión a través del mismo método de derivación de llaves utilizando el mismo modo de derivación de llave y familia de la función pseudoaleatoria en cada operación de expansión.

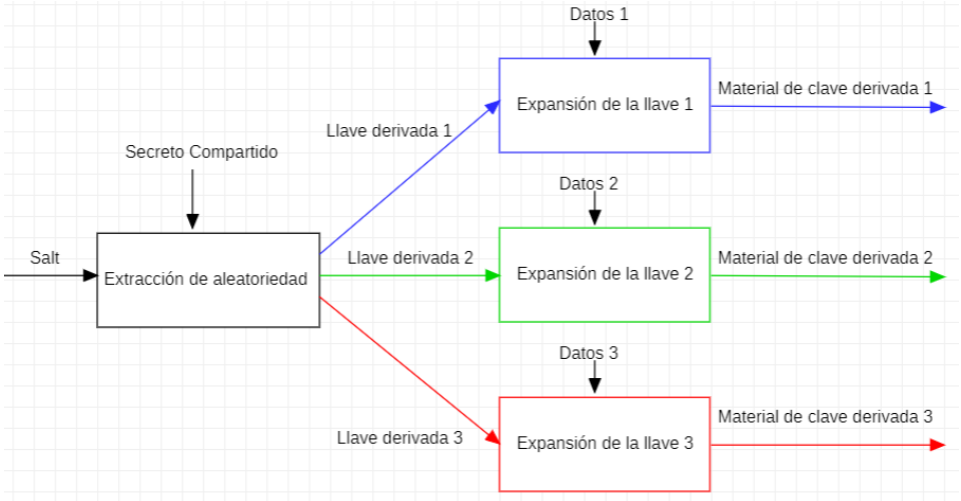

Figura 34: Proceso de expansión de llaves

Fuente: NIST Special Publication 800-56C Revision 2.

Para aplicar las recomendaciones en aplicaciones existentes con funciones de derivación de llaves ver SP 800-135 Revision 1.

3) Llave simétrica generada usando esquema de acuerdo de llaves

Si dos entidades comparten un mismo esquema de acuerdo de llaves dentro de un mismo módulo de generación de llaves entonces pueden establecer la llave simétrica a través de este medio. Esto da como resultado una llave que comparten las entidades participantes en la transacción de acuerdo de llaves.

NIST clasifica los esquemas de acuerdo de llaves en dos grandes conjuntos según el tipo de aritmética que utilice, los cuales se basan en logaritmos discretos (ver SP 800-56 A) y factorización entera (ver SP 800-56B). Además, se incluyen recomendaciones para los métodos de derivación de llave en los esquemas de establecimiento de llaves en SP 800-56C.

Independientemente del tipo de esquema de acuerdo de llave que se utilice se tienen tres fases definidas.

- Preparación para establecer la llave

  El propietario del par de llave es la entidad autorizada para usar la llave privada cuyos requisitos se basan en el tipo de esquema de establecimiento de llaves, además del tipo de llaves que se generen siendo estas estáticas o efímeras.

  Como primer paso se debe obtener/definir los parámetros de dominio de una lista aprobada (ver SP 800-56Ar3 Apéndice D) o generarlas como se especifica a través de un ente de confianza.

  Si el par de llaves se genera por un ente de confianza este debe transportarlas al propietario proveyendo autenticación de fuente y protección a la integridad de tales llaves.

  Si el esquema de establecimiento de llaves requiere de una llave efímera, el propietario debe generarla tan cerca sea posible al tiempo de su uso.

  Se debe un identificador único a la entidad propietaria del par de llaves, de manera que se pueda diferenciar de las otras entidades

- Proceso de acuerdo de llave

  Este proceso varía según el esquema de acuerdo de llave seleccionado, por lo tanto, se recomienda la guía de esquemas aprobados por NIST en SP 800-56Ar3.

  Algunos esquemas de acuerdo de llaves generan pares de llaves efímeras de las cuales se brinda la llave pública a las demás entidades y la privada nunca se comparte.

  Otros esquemas requieren la generación de un *nonce* y proveerlo a las demás entidades.

  Según las circunstancias, alguna información pública adicional puede proveerse o brindarse a las demás entidades.

  Además, si alguna entidad participante en la transacción del acuerdo de llave requiere evidencia sobre si una determinada organización ha computado el mismo secreto o derivado el mismo material clave secreto se ejecuta según se determina en SP 800-56Ar3.

- Proceso de transporte de la llave

  En este proceso una entidad (el emisor) selecciona un valor para el material de clave secreta y, posteriormente, la distribuye de forma segura a las demás entidades (los receptores).

  El transporte de la llave puede hacerse a través de los algoritmos y llaves de envoltura de llave aprobados por NIST (ver SP 800-38F). A continuación, se mencionan los algoritmos aprobados actuales:

Algoritmo	**Texto en plano**	**Texto cifrado**	**Motivo del límite máximo**
KW (AES Key Wrap)	2 a 2^{54} – 1 semibloques	3 a 2^{54} semibloques	Ver requerimientos en SP 800-38F Apéndice A.4
KWP (AES Key Wrap With Padding)	1 a 2^{32} – 1 octetos	2 a 2^{29} semibloques	Indefinido sobre otras longitudes

TKW (TDEA Key Wrap)	2 a 2^{28} – 1 semibloques	3 a 2^{28} semibloques	Ver requerimientos en SP 800-38F Apéndice A.4

Tabla 45: Funciones de envoltura de llaves

Fuente: NIST Special Publication 800-38F December 2012.

Se debe tener siempre presente que las propiedades de seguridad en el proceso de establecimiento de llaves dependen de:

- El esquema de acuerdo de llave.
- El algoritmo de envoltura de llave.
- El protocolo de comunicación que se utiliza.

Antes de ejecutar el transporte de la llave, el emisor debe utilizar la llave pública del destinatario para tener garantía de su validez. Para realizar tal procedimiento se utilizan los métodos aprobados en el SP 800-56Br2:

- Garantía de la validez de la llave pública de la otra entidad antes de usarla en la transacción de establecimiento de llave con su supuesto propietario (y su uso).
- Garantía que a supuesta llave pública del propietario (la otra entidad) posea la llave privada correspondiente a la pública.

Para ahondar en este tema se recomienda seguir las pautas indicadas por NIST en SP 800-56Br2 apartado Assurances Required by a Public-Key Recipient.

4) Llave simétrica derivada a partir de una llave preexistente

Es muy común ver que las llaves simétricas se deriven utilizando una función de derivación de llaves y una llave preexistente conocida como llave para la derivación de llaves. La llave preexistente puede haber sido:

- Generada a través de un generador de *bits* aleatorios aprobado.
- Acordada mediante un esquema de acuerdo de llaves.
- Derivada utilizando un método/función y una llave preexistente(diferente).
- Una función aprobada de múltiples llaves criptográficas.

5) Llave simétrica derivada a partir de una contraseña

Otra manera de generar una llave simétrica es a partir de una contraseña o frase de acceso.

Cuando una llave se genera a partir de una contraseña o frase de acceso, la entropía proveída se considera cero a menos que esta contraseña se haya generado a través de un generador de *bits* aleatorios aprobado por NIST.

El material clave derivado de una función de derivación de llave a partir de una contraseña se llama llave maestra (*master key* en inglés), la cual se usa para:

- Generar una o más Data Protection Keys (DPK) o llaves de protección de datos para proteger otros datos.
- Generar una llave intermedia para proteger una o más DPK existentes o que se generan a partir de una llave maestra usando una función de derivación de llaves aprobada.

Nota. La llave maestra no debe utilizarse para otros propósitos diferentes a los que se indican en los puntos anteriores.

Según se indica en SP 800-132, una función de derivación de llaves con base en contraseña (PBKDF) tiene como parámetros la contraseña, la longitud de la llave y el *salt*. Esto da como resultado una llave maestra como se muestra en la siguiente figura:

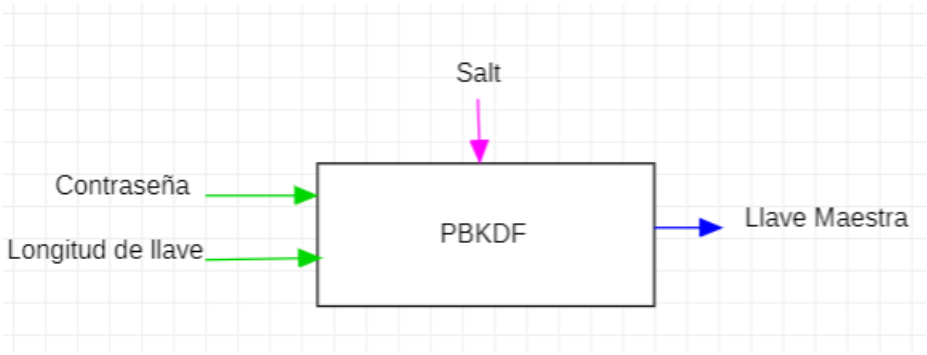

Figura 35: Función PBKDF

Fuente: SP 800-132.

6) Llave simétrica producida por la combinación de múltiples llaves y otros datos

Cuando un conjunto de llaves simétricas K_1, K_2... K_n se generan o se establecen independientemente, después pueden combinarse dentro de un módulo de generación de llaves con el objetivo de formar una llave definitiva.

Además, otros datos de información (D_1, D_2... D_m) pueden también utilizarse en la combinación junto con las K_i para formar la llave definitiva en condiciones específicas. En este caso, mientras que los valores de K_i deben ser secretos, lo mismo no es estricto para los valores de D_i.

Cada K_i es generada o establecida de manera independiente a través de métodos aprobados (listados posteriormente) para que soporten una seguridad igual o mayor que la seguridad que se planteó para la fuerza del algoritmo o aplicación que depende del resultado de la llave definitiva. Además, cada K_i solo debe utilizarse para la computación de una llave simétrica específica y queda totalmente desaconsejado otro propósito para estas.

Cabe destacar que, ningún valor del conjunto de K_i depende de otro valor del mismo conjunto, por lo tanto, no es factible utilizar el conocimiento de cualquier valor K_i para obtener información sobre otros valores K_i.

De igual manera, los valores del conjunto K_i no dependen de los valores D_j, por lo tanto, el conocimiento de cualquier valor D_j no permite utilizarse para obtener información sobre los valores K_i.

A continuación, se listan los métodos aprobados para combinar las llaves (K_i) y otros datos (D_j).

- Concatenamiento de dos o más valores K_i:

  $K = K_1 \,||\, \ldots \,||\, K_i$

  En donde se delimitan las siguientes pautas.

  a) El método requiere de $i \geq 2$.
  b) La suma de la longitud de bits de los valores de K_i es igual a la longitud requerida para la llave definitiva.
  c) El método que se utiliza para generar o establecer los valores de la llave definitiva deben cumplir con que la suma de la mínima entropía proveída por este método sea igual o mayor que la mínima entropía requerida para la generación de la llave definitiva.

- Operación XOR exclusivo de una o más llaves simétricas y (si requerido) uno o más datos:

  $K = K_1 \oplus \ldots \oplus K_i \oplus D_1 \oplus \ldots \oplus D_j$

  En donde se delimitan las siguientes pautas.

a) La longitud de cada valor K_i y de cada D_j es igual a la longitud de bits requerida para la llave definitiva.
b) Los métodos usados para generar o establecer los valores K_i deben, al menos uno, proveer entropía igual o mayor que la requerida para la llave definitiva.

- Un proceso de extracción de claves:

$$K = T(\text{HMAC-hash}(salt, K_1 \,||\, \ldots || \, K_i \,||\, D_1 \,||\, \ldots || \, D_j), K_{Longitud})$$

En donde se delimitan las siguientes pautas.

a) Las funciones HMAC-hash deben implementar las HMAC aprobadas (ver FIPS 198) con la certeza de que cumpla o exceda la seguridad del algoritmo o aplicación que depende de la llave resultante (ver SP 800-57 part 1).
b) La longitud del *salt* debe ser igual o mayor que 0 y debe ser conocido por todas las entidades que utilicen este proceso de extracción para obtener el mismo valor para la llave definitiva.
c) El método requiere que $i \geq 1$. Si $i = 1$ entonces $K_1 \,||\, \ldots \,||\, K_n$ es solo K_1.
d) Este método requiere que $m \geq 0$.
   Si $m = 0$ entonces $D_1 \,||\, \ldots \,||\, D_m$ es un *string* vacío.
   Si $m = 1$ entonces $D_1 \,||\, \ldots \,||\, D_m$ es justo D_1.
e) T es una función de truncamiento, la cual se define como:
   T(x, l) = Truncamiento de la cadena de *bits* x a los l *bits* más a la izquierda de x, donde l ≤ la longitud de x en *bits*.
f) La longitud del bloque de salida de la función *hash* usada con HMAC es al menos a la longitud de *bits* de la llave definitiva.
g) La suma de las mínimas entropías proveídas por los métodos que se utilizan para generar o establecer los valores K_i son igual o mayor que la mínima entropía requerida para la salida de la llave definitiva.
h) Órdenes alternativos se permiten cuando se forman las concatenaciones de los valores K_i y los datos, sin embargo, este orden debe ser conocido por las demás entidades computando el valor de la llave definitiva.
i) La fuerza de seguridad de la llave formada por la combinación de los múltiples valores K_i y datos es sujeta a las consideraciones expresadas en SP 800-133r2 sección Supporting a Security Strength.

5.6.2 Distribución

Las llaves asimétricas que se generan dentro de un módulo de generación de llaves con frecuencia precisan ser compartidas con una o muchas otras entidades, las cuales poseen sus propios módulos criptográficos.

Las llaves simétricas pueden ser distribuidas de forma manual o utilizando un método de transporte de llave o de envoltura de llave. Los módulos criptográficos aprobados son los que se discuten en la publicación FIPS-140.

Los métodos aprobados (ver SP 800-133r2) se detallan a continuación:

- Métodos de transporte de llaves

  Este tipo de método se divide principalmente en dos grandes conjuntos. En primer lugar, se tiene el esquema de acuerdo de llaves y, en segundo lugar, el esquema de transporte de la llave

  En este tipo de esquema existen dos entes involucrados: el emisor y el receptor de la llave, además, el material clave establecido lo selecciona el emisor. Es frecuente (aunque no obligatorio) el uso de información adicional en el proceso de transporte de llave con el objetivo de asegurar que el material clave se ligue adecuadamente al contexto de la transacción del transporte de esta llave.

  Se debe tener claro que cada una de las entidades en la transacción de transporte de llave debe saber cada una de la información adicional y su formato. Además, debe requerirse utilizar esta información a tiempo para su uso según lo defina el esquema que se emplea.

  - Esquema de acuerdo de llaves

    Con base en SP 800-56Br2, se recomienda la familia de esquemas KAS1 y KAS2:

Esquemas de KAS1	
KAS1-basic	Esquema básico sin confirmación de llave.
KAS1-Party_V-confirmation	Variante de KAS1-basic con confirmación de llave unilateral proveída por la entidad receptora hacia la organización emisora.

Tabla 46: Esquemas KAS1

Fuente: NIST Special Publication 800-56B Revision 2.

Esquemas de KAS2	
KAS2-basic	Esquema básico sin confirmación de llave
KAS2-Party_V-confirmation	Variante de KAS2-basic con confirmación de llave unilateral proveído por la entidad receptora a la organización emisora.
KAS2-Party_U-confirmation	Variante de KAS2-basic con confirmación de llave unilateral proveída por la entidad emisora a la organización receptora.
KAS2-bilateral-confirmation	Variante de KAS2-basic con confirmación de llave bilateral proveída entre las entidades emisora y receptora.

Tabla 47: Esquemas KAS2

Fuente: NIST Special Publication 800-56B Revision 2.

Para tener un panorama más amplio sobre el funcionamiento e implementación de cada uno de los esquemas de KAS1 y KAS2 se recomienda seguir las pautas indicadas en SP 800-56Br2.

- Esquema de transporte de llaves

Con base en SP 800-56Br2, se recomienda la familia de esquemas KTS-OAEP:

La familia KTS-OAEP se basa en las operaciones RSA-OAEP (ver SP 800-56Br2). En estos esquemas se sigue la siguiente forma:

a) La entidad emisora encripta el material clave (y datos adicionales) por transportarse utilizando la operación RSA-OAEP.ENCRYPT y la llave pública de establecimiento de llaves de la organización receptora para producir un texto cifrado y, posteriormente, enviarlo a la entidad receptora.

b) La entidad receptora desencripta el texto cifrado utilizando su llave privada de establecimiento de llave y la operación RSA-OAEP.DECRYPT para recuperar el material clave transportado.

c) Si la confirmación de llave está incorporada entonces el material clave transportado se divide en dos partes: la MacKey y la KeyData. Cada entidad computa su etiqueta MAC, la cual debe ser la misma para todas las partes. En el caso de la organización receptora le envía su valor obtenido de la operación sobre la MAC y si ambas coinciden entonces se envía la confirmación a la entidad receptora.

Nota. El transporte de la llave puede llevarse a cabo a través de los esquemas de establecimiento de llaves utilizando un algoritmo aprobado de envoltura de llaves (ver SP 800-38F) para agregar propiedades de seguridad híbridas en el proceso de establecimiento de llaves, el cual depende del esquema de establecimiento de llave elegido.

- Métodos de envoltura de llaves

Los esquemas de envoltura de llaves con base en AES descritos en el SP 800-38F son los siguientes:

Algoritmo	Texto en plano	Texto cifrado	Motivo del límite máximo
KW (AES Key Wrap)	2 a 2^{54} – 1 semibloques	3 a 2^{54} semibloques	Ver requerimientos en SP 800-38F Apéndice A.4
KWP (AES Key Wrap with Padding)	1 a 2^{32} – 1 octetos	2 a 2^{29} semibloques	Indefinido sobre otras longitudes
TKW (TDEA Key Wrap)	2 a 2^{28} – 1 semibloques	3 a 2^{28} semibloques	Ver requerimientos en SP 800-38F Apéndice A.4

Tabla 48: Funciones de envoltura de llaves

Fuente: NIST Special Publication 800-38F December 2012.

- Método manual

Cuando se comparten las llaves de forma manual se deben proteger las llaves secretas, llaves privadas y secciones de llaves a través de envoltura de llaves (encriptación con protección de integridad) o distribuirlas usando procedimientos de seguridad físicos apropiados.

Si se utiliza el procedimiento de conocimiento dividido para la distribución entonces cada parte de la llave debe distribuirse de forma separada. Existen ciertos procesos que se deben seguir cuando se opta por la distribución manual, los cuales se listan a continuación:

a) El material clave debe distribuirlo una fuente autorizada.
b) Cualquier entidad que distribuya material clave en texto plano es de confianza tanto para la organización que genera el material clave como para cualquier entidad que la recibe.
c) El material clave es protegido de acuerdo con SP 800-57 part 1 Revision 5 sección 6.
d) El material clave lo reciben destinatarios autorizados.

Cuando se distribuye de forma encriptada se deben utilizar esquemas de envoltura de llaves o llave de envoltura de llaves aprobados y se utiliza únicamente para tal fin. Si se decanta por procedimientos de seguridad físicos se debe contar con el nivel de seguridad apropiado, los cuales se vuelven mucho más críticos cuando se distribuye material clave secreto en forma de texto plano.

5.6.2 Llaves asimétricas

El par de llaves debe generarse de acuerdo con las especificaciones matemáticas aprobadas, establecidas tanto por NIST como de FIPS.

5.6.2.1 Generación

La generación del par de llaves se puede llevar de las siguientes formas:

- Para llaves estáticas:
  - La entidad propietaria del par de llaves (por ej.: la organización que utiliza la llave privada para realizar computación criptográfica).

- Una instalación central de generación de llaves que distribuye el par de llave (se explica en el apartado de distribución).
- El propietario y la instalación en un proceso en conjunto.

- Para llaves de firma digital
  - El propietario del par de llaves estáticas las genera para sí mismo, no compartiendo la llave privada a las demás entidades a excepción de que el propietario sea una entidad. En ese caso, es aceptable que la llave privada se comparta entre las subentidades del propietario, ya que estas representan al propietario original.
- Llaves efímeras
  - Las claves efímeras se utilizan a menudo para el acuerdo de claves en lugar o además del uso de claves estáticas. Este tipo de llaves se genera por cada nueva transacción en el establecimiento de llaves (ver SP 800-56 A).

5.6.2.2 Distribución

Para la distribución se tienen tres conjuntos según se indica en SP 800-57 part 1 Revision 5.

- Distribución de llaves públicas

Las llaves públicas estáticas tienen larga vida y, a la vez, se usan para realizar múltiples ejecuciones con el mismo algoritmo. Por otro lado, las llaves públicas efímeras tienen vida corta y se usan en una única ejecución con el mismo algoritmo.

La distribución de este tipo de llaves tiene el objetivo de proveer la garantía al receptor de estas llaves sobre la veracidad del propietario y, de esta manera, validar su identidad.

Existen algunos otros fines para la distribución de la llave pública que proveen garantía al receptor:

a) El propósito/uso de la llave es completamente conocido (ej., firmas digitales RSA o acuerdo de llaves de curvas elípticas).
b) Todos los parámetros asociados con la llave se conocen plenamente (por ej., parámetros de dominio).
c) La validez de la llave (por ej., la llave satisface las propiedades aritméticas requeridas).

d) El propietario posee la correspondiente llave privada.

A continuación, se detallan las posibles maneras de distribuir las llaves públicas.

- Distribución de la clave pública de un anclaje de confianza en una PKI:

  La llave pública de una autoridad certificadora (AC) es el fundamento en el que se basan todos los servicios con base en la infraestructura de llave pública (PKI del inglés *public key infrastructure*).

  La llave pública del anclaje de confianza no es un secreto, sin embargo, el tema de la autenticidad de esta llave es crucial para este tipo de infraestructura.

  Este tipo de llave pública puede obtenerse de distintas maneras según mecanismo que se utilice, lo cual proveerá diferentes niveles de garantía. Los mecanismos que se utilizan pueden depender del rol de la entidad en la infraestructura. Este tipo de llaves públicas se usan para distintos fines como:

  a) Certificados autofirmados root-CA X.509.
  b) Embebidos dentro de aplicaciones y distribuidas como un solo paquete.
  c) Validación de otras certificaciones o de sitios en el sistema operativo.
  d) Validaciones de certificados TLS presentes en los protocolos TLS en sitios web.

  Para mayor detalle sobre el flujo del proceso de distribución de este tipo de llaves públicas se recomienda ver NIST SP 800-57 Part 1 Revision 5.

- Presentación ante una autoridad de registro o de certificación:

Estas llaves públicas las provee una autoridad certificadora (AC) o las registra una autoridad registradora (AR) para posteriormente obtenerla de una autoridad certificadora. Durante este proceso de registro, tanto la AR como la AC deben obtener por parte del futuro propietario de la llave los datos correspondientes

para dar garantía de la autenticidad del propietario de la llave o representante autorizado.

Además de los datos del futuro propietario de llave, también se requiere establecer el uso que se le dará a la llave junto con cualquier parámetro requerido. Existen ocasiones en donde se permite la propiedad anónima de las llaves, en este caso se utiliza un seudónimo como identificador, el cual es único para su nombramiento.

La fuerza de la seguridad en la que se basa la infraestructura depende directamente del método que se utiliza para distribuir la llave a una AR o AC como los que se mencionan a continuación:

a) Los datos necesarios para asegurar la autenticidad de la llave pública los provee en persona el futuro propietario o un representante autorizado del propietario (por ej., una organización, dispositivo o proceso).
b) La identidad del futuro propietario o de un representante autorizado se establece y su autorización la verifica personalmente una AR o AC a través del registro de identidad.
c) La identidad del futuro propietario se establece en la AR o AC a través de una determinación previa de la identidad del propietario.
d) Tanto la llave pública como su uso, parámetros, información de garantía de validez y garantía de posesión las provee la AR o AC junto con una identidad reclamada para el propietario y la autorización para recibir un certificado.
e) La llave pública y la dirección DNS incluidas en el campo de nombre común o nombre alternativo del sujeto del certificado se proveen sobre la conexión del AR vía solicitud de firma de certificado.

- Distribución general de claves públicas estáticas:

  Este tipo de llaves se distribuyen a entidades distintas de una AR o AC de muchas maneras:

  a) Distribución manual de la llave pública por el propietario o por el representante del propietario, es decir, transferencia de cara a cara o a través de un mensajero de confianza.
  b) Distribución manual o automatizada de la certificación de llave pública por el propietario, el representante del propietario, la AC o por un repositorio de certificados.
  c) Distribución automatizada de la llave pública utilizando, por ejemplo, un protocolo de comunicación que provea garantía de autenticación e integridad del contenido.

  Para profundizar sobre estos tipos de distribución de llaves públicas se recomienda ver NIST SP 800-57 Part 1 Revision 5.

- Distribución de llaves públicas efímeras

  Cuando se utilizan las claves públicas efímeras se distribuyen como parte de un protocolo seguro de acuerdo de claves cuyo proceso puede estar compuesto por:

  - El esquema de acuerdo de llaves
  - El protocolo
  - La llave de confirmación
  - Cualquier negociación asociada
  - El procesamiento local

  Los puntos anteriores deben combinarse, de manera que provean al destinatario con la garantía suficiente para indicar el emisor correspondiente. El destinatario de la llave pública efímera debe tener la garantía de validez de la llave con base en los puntos indicados en SP 800-56 A Revision 3 sección Recipient Assurance of Ephemeral Public-Key Validity, antes del uso de esta llave en el proceso de acuerdo de llaves.

- Distribución de par de llaves que se generan de forma centralizada

  El par de llaves estáticas pueden generarse a través de:

  1) Un módulo criptográfico aprobado (ver FIPS 140-3).

  2) Instalación central de generación de llaves para sus suscriptores.

  Cuando se genera la llave privada del par de llaves utilizando una instalación central, esta debe distribuirse únicamente al propietario solicitante o a un representante legal para su instalación. En este proceso de generación de llaves se debe asegurar la confidencialidad de la llave privada y el proceso de distribución debe proporcionar la autenticación de la identidad del destinatario y la autorización establecida durante el proceso de registro de la entidad.

  La distribución de las llaves hacerse de las siguientes maneras (aunque no se limita):

  - Manual
    a) Mensajería
    b) Correo físico
    c) Entrega personalmente
    d) Cualquier otro medio indicado por la instalación central de generación de llaves.
  - Método automático seguro
    a) Protocolo de comunicación seguro

El propietario del par de llaves puede obtener la garantía de la validez sobre la asociación de ambas llaves, por ejemplo, al validar que son consistentes al encriptar con la llave pública posteriormente se puede desencriptar con la llave privada. Para profundizar los métodos de validación de llaves se recomienda ver SP 800-56 A, SP 800-56B y SP 800-89.

5.7 Transición a nuevos algoritmos y llaves criptográficas

Cuando se habla de la estimación de la fuerza de seguridad en criptografía se hace referencia a la asociación entre el algoritmo y la longitud de la llave en cuanto a la proyección del tiempo de vida que se espera que tanto el algoritmo como la longitud

de la llave pueda proveer de una adecuada seguridad. Además, se debe tener siempre presente que el tamaño de la llave criptográfica es una parte fundamental para lograr estas determinaciones.

Otra manera de referirse a la fuerza de seguridad es sobre la medida de la dificultad de reversar la protección criptográfica (por ej., descubriendo la llave) utilizando computadoras clásicas. De esta manera, cada algoritmo criptográfico con una determinada longitud de llave puede proveer siempre y cuando esta llave contenga el suficiente nivel de entropía.

Sin embargo, al pasar del tiempo, la fuerza de seguridad que proveen los algoritmos o llaves puede verse reducida y, en algunas ocasiones, totalmente perdida debido a las capacidades del poder computacional creciente y el criptoanálisis. Es debido a este panorama que se debe implementar nueva protección a los datos a través de algoritmos y llaves criptográficas más fuertes.

Un punto importante de tener en cuenta es que la información que fue protegida previamente utilizando un algoritmo y llave no adecuada (en la actualidad) puede ser no segura. Por lo tanto, debe hacerse una transición para proteger estos datos antiguos y los nuevos en donde se pueden incluir otras llaves o información sensible.

Si existe una reducción en cuanto a la fuerza de seguridad que provee un algoritmo o llave criptográfica pueden producirse las siguientes implicaciones:

- Información encriptada:

  La seguridad de la información encriptada que fue disponible (por cualquier motivo) en algún momento para una entidad no autorizada en su forma encriptada debe considerarse sospechosa.

  Un gran ejemplo para este caso es una llave que se transmitió de manera encriptada (utilizando una llave de envoltura o una llave de transporte y un algoritmo o longitud de llave que posteriormente fue vulnerada) puede necesitar considerarse debido a que cualquier adversario pudo haber guardado la forma encriptada de la llave para posteriormente desencriptarla si en algún momento existe la posibilidad de poder quebrar el algoritmo. Aún incluso si la información encriptada que se transmitió se encripta nuevamente para su almacenamiento

usando un algoritmo o llave distinta, esta información puede ser todavía comprometida debido a la debilidad del algoritmo o llave de transmisión.

Por otro lado, si la información que fue encriptada con un algoritmo o llave que ya no brinda la fuerza necesaria para considerarse segura y esta información no fue transmitida en ningún momento entonces se puede considerar todavía segura. Sin embargo, se recomienda la transición a un algoritmo o llave con más fuerza de seguridad por si es posible la salida de esta información del lugar seguro en el que se encuentra por cualquier motivo.

Algunas recomendaciones se listan a continuación:

- El mecanismo de encriptación que utiliza la información que está disponible para entidades no autorizadas en su forma encriptada debe proveer un nivel alto con respecto a la protección de la seguridad requerida.
- El uso de cada llave debe ser limitado (un criptoperiodo corto) para que en el caso de que esta llave sea vulnerada no revele demasiada información.
- Encriptar la información por segmentos con distintas llaves para que si alguna se vulnera o incluso el algoritmo tiene una vulnerabilidad entonces el adversario tiene que esforzarse más para obtener una mínima cantidad de información.

- Firmas digitales en los datos almacenados que se transmitieron originalmente:

  Las firmas digitales pueden computarse sobre los datos antes de ser transmitidas y, posteriormente, almacenadas. En esta situación, tanto los datos firmados como la propia firma digital serían almacenados.

Si por cualquier motivo la fuerza de la seguridad de la firma se ve reducida después (quizás por el rompimiento del algoritmo criptográfico o porque un adversario determinó la llave), la firma puede considerarse todavía válida. Esto con la condición de que los datos almacenados y sus firmas digitales asociadas hayan sido protegidas adecuadamente de modificaciones desde un tiempo antes de que se haya encontrado el decrecimiento de su fuerza (por ej. al aplicar una firma digital utilizando un algoritmo o llave más fuerte).

- Códigos de autenticación simétrica en los datos almacenados que se transmitieron originalmente:

  Los códigos de autenticación simétricos (como MAC, por ejemplo) pueden computarse sobre datos antes de transmitirse o (posteriormente) almacenarse. En el caso de que los datos y el código de autenticación sean almacenados y recibidos y después la fuerza de seguridad del algoritmo o de la llave se reduce (por ej., debido al quiebre del algoritmo), el código de autenticación que se utiliza puede considerarse todavía válido con la salvedad de que los datos y su código de autenticación asociado hayan sido protegidos de manera correcta de modificaciones antes del decrecimiento de su fuerza (por ej., al aplicar otro código de autenticación utilizando un algoritmo o llave más fuerte).

Debido a lo anterior, se debe contar con una buena estrategia para realizar la transición a algoritmos o llaves más robustas que proporcionen más seguridad que satisfaga las necesidades del momento. Un buen enfoque es aquel que apunta a la flexibilidad en donde tanto implementaciones como aplicaciones puedan adoptar de manera sencilla y rápida nuevas ofertas de seguridad criptográficas, lo que conduciría a la mejor solución en cualquier momento.

Un aspecto que se debe tener siempre presente cuando se trabaja con criptografía es que todo se estima en cuanto a la fuerza de seguridad que tanto los algoritmos como las propias llaves criptográficas brindan. Con esto se pretende dar a

entender que lo que ahora mismo es seguro quizá en poco tiempo ya no lo sea (30 minutos, una semana, dos meses, 4 años, etc.). Por esto, se trabaja con estimaciones, ya que nadie tiene certeza del tiempo exacto en el que la seguridad actual ya no sea tan segura como para continuar brindando el servicio deseado.

El periodo estimado en el cual los datos protegidos a través de un algoritmo criptográfico (y tamaño de llave) permanecen seguros se denomina vida útil de la seguridad del algoritmo. Durante este tiempo, el algoritmo puede utilizarse para procesos, tanto para aplicar protección criptográfica como para procesar la información protegida.

Una práctica bastante extendida es la de establecer un periodo más corto para la protección de los datos que la propia vida útil de la seguridad del algoritmo, no obstante, se espera que el algoritmo provea de protección adecuada durante toda su vida útil. A continuación, se muestra el periodo de vida segura de un algoritmo criptográfico:

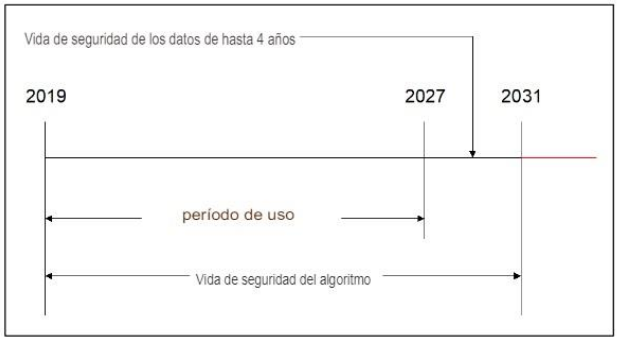

Figura 36: Periodo de uso por el originador del algoritmo

Basado: NIST Special Publication 800-57 Part 1 Revision 5.

Para seleccionar un nuevo servicio criptográfico para una aplicación determinada, se debe verificar la vida útil de la seguridad del algoritmo y la vida de seguridad de los datos por proteger y, posteriormente, un algoritmo y tamaño de llave que se adecúe a las necesidades de los requerimientos que se plantearon. Una vez que se hayan seguido los pasos anteriores se debe establecer un sistema para la gestión de la llave.

Siempre se debe contar con un plan definido para cuando se determine que un algoritmo o tamaño de llave no proporciona la protección que se desea para la información y realizar la transición a nuevos algoritmos o tamaño de llaves aprobados y con tiempo de vida para proteger los datos que se ajuste a las necesidades presentadas.

En ninguna circunstancia se recomienda implementar y mucho menos utilizar algún algoritmo o tamaño de llave que se haya marcado como no apto para los procesos de encriptación de los datos. Lo anterior debido a que existe un gran riesgo sobre la confidencialidad de los datos si estos son comprometidos.

No obstante, cuando se realiza el proceso de transición a un nuevo algoritmo y tamaño de llave, se debe destacar que no siempre tomar el tamaño más grande (innecesariamente larga) es la mejor opción, ya que puede acarrear efectos adversos en cuanto a rendimiento.

El proceso de transición puede tener el grado de complejidad variante según los factores que afecten su elección. Puede ser tan sencillo como seleccionar una opción de algoritmo o llave más segura que se adecúe a las necesidades del sistema actual o tan complejo como construir un nuevo sistema completamente.

Además, las ramificaciones propias de la transición dependen de la escala en donde se implementa, es decir, no es lo mismo realizar la transición de un nuevo algoritmo y tamaños de llaves en un único sistema de almacenamiento que realizarlo para cumplir con las necesidades de un cambio total para implementar TLS o SSH en donde existirán muchas más implicaciones y todo recaerá sobre las necesidades propias de cada uno y queda fuera del alcance de esta investigación. Para finalizar, se deben tomar en cuenta los siguientes puntos cuando se haga la transición a nuevos algoritmos y tamaños de llaves:

1) Validar la sensibilidad de información por proteger y la vida útil del sistema.
2) Seleccionar algoritmos y tamaños de llaves aprobados que satisfagan los requerimientos establecidos.
3) Evaluar antes de la implementación para considerar la eficacia y seguridad proporcionada por la nueva criptografía por implementar.
4) Realizar pruebas al sistema con la nueva implementación del nuevo algoritmo o tamaño de llave antes de ponerlo en producción.
5) Se debe implementar de manera que la transición del viejo sistema al nuevo sea lo más transparente posible.
6) Se deben realizar evaluaciones después de la implementación para validar que todos los requerimientos se abordan con éxito y el sistema proporcione el servicio como antes lo realizaba.

Capítulo 6. Conclusiones y recomendaciones

6.1 Conclusiones

En la actualidad, la criptografía desempeña un rol muy importante en la vida y los quehaceres diarios en el mundo digital en el cual las personas se desarrollan de forma directa o indirectamente. Sin embargo, es un tema complejo aparte de la diversidad de algoritmos existentes con sus múltiples ventajas y servicios que se brindan, lo cual puede amedrentar a quienes se la topen en los procesos que se relacionan con la adicción de seguridad en entornos computacionales y, por lo tanto, se debe contar con mucha experiencia para intentar establecer la solución a un determinado problema.

Debido a lo anterior y con base en los objetivos planteados es que la propuesta actual compacta de manera integral y ordenada siete grandes áreas críticas, que corresponden al análisis, determinación y selección de los algoritmos y llaves criptográficas. Esto según las diferentes necesidades que se pueda tener en cuanto a protección en el mundo digital y los servicios prestados por cada algoritmo.

Aun sabiendo que la criptografía digital es una de las mejores defensas en cuestiones de seguridad en los activos digitales, las entidades y empresas no le brindan la importancia con énfasis en aquellas pymes (pequeña y mediana empresa) en donde la criptografía queda relegada, incluso si estas son compañías que se relacionan con la informática.

Por lo tanto, como se observó, no existe un único camino por seguir para seleccionar la mejor solución para un determinado problema, por lo que el modelo de selección de algoritmos criptográficos es esencial para esta labor a través de la identificación de aquellos algoritmos aprobados por NIST indicados en sus múltiples publicaciones especiales. Se excluye a todo aquel algoritmo que no se encuentre apto para brindar seguridad a procesos criptográficos para las organizaciones gubernamentales estadounidenses, las cuales son el centro de atención tanto para NIST, FIPS y muchas otras entidades que se mencionaron a lo largo de la propuesta.

Antes de siquiera empezar a ver temas de criptografía se realizó una guía para determinar los entornos informáticos y la forma de identificar el estado en el que están los datos para concientizar el nivel y el tipo de seguridad que se recomendaría seleccionar para su protección adecuada.

Aparte de conocer los algoritmos simétricos y asimétricos incluyendo curvas elípticas aprobados actualmente por las más grandes organizaciones establecedoras de estándares internacionales, lo que incluye la criptografía, también se hizo énfasis sobre las características que brindan, tanto por los propios algoritmos como por las llaves y otros componentes. A partir de esto se determina que estas características hacen del modelo de selección de algoritmo una alternativa sumamente relevante en el momento de elegir la protección con base en los servicios que brinda cada algoritmo y llave.

La eficacia de los algoritmos y llaves tratadas en la investigación es el tema primordial. Debido a esta relevancia, se han hecho las debidas recopilaciones, análisis y sintetización de las pautas sobre la seguridad de los algoritmos y su tiempo de eficacia, así como su fuerza de protección estimada a través de los múltiples documentos sugeridos por NIST y FIPS para los siguientes años y se tiene en cuenta el poder computacional creciente.

Además, se han recopilado las recomendaciones pertinentes para cada fase del modelo de selección de algoritmos para inculcar las mejores prácticas en temas de seguridad para aplicar la protección de forma adecuada con base en las pautas que brindan organizaciones de la talla de NIST, FIPS, OWASP, entre otros.

El conocer los algoritmos y llaves criptográficas para abordar una determinada necesidad de la mano de grandes organizaciones estandarizadoras de seguridad y referentes mundialmente permite tener un gran respaldo en cuanto a la selección que se tome para ofrecer tranquilidad respecto a la información que se necesite tener asegurada. A la vez, se pueden proporcionar las medidas adecuadas para realizar la transición en el caso de nuevos algoritmos o longitudes de llave, lo cual ofrece flexibilidad y buena resiliencia en los entornos informáticos en donde se aplique.

Se aborda la investigación para instar a los profesionales a utilizar algoritmos y llaves criptográficas aprobadas actualmente y seguir las medidas indicadas por las organizaciones para blindar con seguridad los datos en juego. De esa manera, se evitan altercados con temas de confidencialidad, integridad y disponibilidad de estos datos a través de un modelo inteligente de selección de algoritmos criptográficos modernos.

6.2 Recomendaciones

A continuación, se listan algunas recomendaciones fundamentadas especialmente en la experiencia obtenida a través del desarrollo del presente trabajo investigativo en donde se abordan temas como estándares, uso del tiempo y costos financieros.

- Con el objetivo de realizar un trabajo de mejor calidad y, si la persona investigadora tiene los recursos financieros suficientes para invertir en otras fuentes para obtener más información, se recomienda que se haga este proceso, ya que existen fuentes investigativas muy buenas, sin embargo, poseen costos para poderlas obtener. Con lo anterior, se insta a tener distintas fuentes para mejorar la calidad del trabajo, esto se debe a que muchos documentos investigativos de pago tienden a ser más completos que los de versiones gratuitas, lo que produce mucho más valor en cuanto a la exactitud y relevancia del tema tratado.
- Se recomienda la consulta a la mayor cantidad de expertos relacionados con el tema de investigación debido a que cuanto más consultas se hagan mayor es la objetividad de la información tratada y, por lo tanto, de lograr un criterio más conciso y acertado al desarrollar la investigación. En caso contrario, cuanto menos consultas se hagan el nivel de objetividad y credibilidad también baja, ya que no se abarca la opinión de aquellos expertos quienes viven diariamente temas y datos importantes que serían vitales para proporcionar en la investigación.
- En cuanto al tiempo y el desarrollo de las tareas referentes al estudio, es importante el tema de la organización. Esto se debe a que la calidad de la investigación mejorará si se cuenta con una definición del tiempo de cada tarea, logrando una estandarización de la calidad proveída.
- Con respecto al instrumento de evaluación, es bastante recomendable realizar una definición sobre las reglas y especificaciones sobre su uso. Esto para que quien lo utilice no tenga la necesidad de corroborar otras fuentes con el objetivo de reafirmar la misma información, excepto que existan nuevas publicaciones especiales en donde se indique alguna modificación referente a la fortaleza de los algoritmos y llaves criptográficas que actualmente se toman en cuenta debido a su aprobación total para usos en procesos criptográficos.

- La implementación de cualquier algoritmo y llave criptográfica, así como cualquier especificación se debe consultar con los documentos oficiales de NIST y FIPS, los cuales se referencian a través de toda la presente investigación para profundizar sobre temas implementativos.

6.3 Recomendaciones y buenas prácticas

6.3.1 Generales

- No se recomienda utilizar de un mismo algoritmo criptográfico para más de un mismo servicio (por ej., confidencialidad, autenticación de la identidad, autenticación de la integridad, autenticación de la fuente, autorización y no repudio).
- No se recomienda utilizar criptografía asimétrica para el proceso de encriptación de grandes cantidades de datos.
- No se recomienda utilizar funciones *hash* solas (sin una llave secreta) para evaluar procesos que se relacionan con integridad.
- Utilizar algoritmos y funciones criptográficas aprobados por NIST y FIPS.
- Utilizar tamaños de llaves aprobados por NIST y FIPS.
- Utilizar generadores de *bits* aleatorios (RBG) aprobados por NIST y FIPS con gran cantidad de entropía para la generación de llaves criptográficas.
- Delimitar el tiempo de vida de las llaves criptográficas.
- El uso de una misma llave para más de un proceso criptográfico diferente puede debilitar la seguridad que se brinda para uno o ambos procesos.
- Limitar el uso de una llave, a la vez, limita el daño que puede ocasionar si la llave se compromete.
- Algunos usos de llaves interfieren con otras llaves.
- Limitar la cantidad de información disponible que pueda revelar la llave.
- Limitar la cantidad de exposición si la llave se compromete.
- Limitar el uso de un determinado algoritmo (tiempo de vida efectivo).
- Seleccionar un RBG que soporte al menos una fuerza de seguridad de 128 *bits* para generar claves.
- Confidencialidad: Cifrar la información utilizando AES-128 y una clave generada por el RBG. Otros tamaños de clave AES también serían apropiados, pero el rendimiento puede ser un poco más lento.

- Protección de la integridad y autentificación de la fuente: Si solo se prefiere una operación criptográfica utilice firmas digitales. Se puede utilizar SHA-256 o una función *hash* mayor para hacer un *hash* de los datos antes de generar la firma. Seleccione un algoritmo para las firmas digitales entre lo que está disponible para una aplicación (por ejemplo, ECDSA con al menos una clave de 256 *bits*). Si hay más de un algoritmo y tamaño de clave disponible, la selección puede basarse en el rendimiento del algoritmo, los requisitos de memoria, etc., rendimiento, requisitos de memoria, etc., siempre que se cumplan los requisitos mínimos.
- Establecimiento de claves: Seleccione un esquema de establecimiento de claves que se base en la aplicación y entorno (véase SP 800-56 A o SP 800-56B), la disponibilidad de un algoritmo en una implementación y su rendimiento. Seleccione un tamaño de clave adecuado para un algoritmo y tamaño de clave que pueda proporcionar al menos 128 *bits* de seguridad. Por ejemplo, si se dispone de un esquema de acuerdo de claves ECC, utilice un esquema ECC y una curva con una clave de 256 *bits* como mínimo. Sin embargo, la clave que se utiliza para el acuerdo de claves debe ser diferente de la clave ECDSA que se emplea para las firmas digitales (ver punto c anterior).
- Longitud de llave que se recomienda: 112, 128, 192, and 256 *bits.*

6.3.2 Criptoperiodos

- Limitar el tiempo disponible para los intentos de penetración de los mecanismos de acceso físico, procedimental y lógico que protegen una clave de la divulgación no autorizada.
- Limitar el periodo dentro del cual la información puede ser comprometida por divulgación inadvertida de una llave criptográfica a una entidad no autorizada.
- Limitar el tiempo disponible para el uso de una determinada llave por los adelantos computacionales en temas de criptoanálisis.
- Si una llave se compromete, su criptoperiodo se considera inválido automáticamente.
- Utilizar criptoperiodos cortos.
- La selección del algoritmo criptográfico y la llave aprobados aumentan la resistencia de los criptoperiodos.

- Las llaves usadas para proteger la confidencialidad de la comunicación tienden a ser más cortas que las llaves usadas para proteger los datos almacenados.
- Los criptoperiodos de los datos almacenados son más largos por la carga del proceso de generación de las llaves y volver a encriptar todos los datos que se encriptaron con llaves antiguas.

6.3.3 Datos relacionados con la criptografía

- Los parámetros de dominio se mantienen en efecto hasta que se modifican.
- Un vector de inicialización (VI) se asocia con la información que ayuda a proteger y es necesario hasta que su forma protegida criptográficamente ya no se necesite.
- Un secreto compartido que se genera durante la ejecución de un esquema de acuerdo de llave es destruido tan pronto como sea necesaria para derivar material de clave.
- Una semilla del generador de *bits* aleatorios (RBG) es destruida inmediatamente después de su uso.
- Otras informaciones públicas no deben ser retenidas más tiempo de lo necesario para procesos criptográficos.
- Otras informaciones secretas no deben ser retenidas más tiempo de lo necesario.
- Un resultado intermedio es destruido inmediatamente después de su uso.

6.3.4 Medidas de protección

- Limitar la cantidad de tiempo que una clave privada secreta simétrica o asimétrica está en forma de texto plano.
- Evitar que los humanos vean las claves privadas simétricas y asimétricas secretas de texto plano.
- Restringir las claves secretas y privadas de texto plano a *contenedores* protegidos físicamente. Esto incluye generadores de claves, dispositivos de transporte de claves, cargadores de claves, módulos criptográficos, módulos de seguridad de *hardware* (HSM) y dispositivos de almacenamiento de claves.
- Utilizar comprobaciones de integridad para garantizar que la integridad de una clave o su asociación con otros datos no ha sido comprometida. Por ejemplo,

las claves pueden estar envueltas (es decir, cifradas e integridad), de manera que las modificaciones no autorizadas de la clave envuelta o a los metadatos de la clave se detecten.

- Emplear la confirmación de la clave para ayudar a asegurar que la clave adecuada fue establecida.
- Establecer un sistema de rendición de cuentas que lleve la cuenta de cada acceso a las claves privadas secretas simétricas y asimétricas en forma de texto plano.
- Proporcionar una comprobación de la integridad criptográfica de la clave (por ejemplo, utilizando una MAC o una firma digital).
- Uso de marcas de tiempo de confianza para los datos firmados.
- Destruir las llaves en cuanto ya no se necesiten.
- Crear un plan de recuperación del compromiso, especialmente en el caso del compromiso de una CA clave.

6.3.5 Plan de recuperación/Compromiso

- La identificación del personal que debe notificar y lo que debe contener la notificación (por ejemplo, el alcance del compromiso-si se comprometieron claves específicas o el proceso de generación de certificados).
- Identificación del personal para realizar las acciones de recuperación.
- El método para obtener una nueva clave (es decir, volver a teclear).
- Un inventario de todas las claves criptográficas (por ejemplo, la ubicación de todas las claves y certificados en un sistema).
- La educación de todo el personal apropiado en los procedimientos de recuperación de compromisos.
- Identificación de todo el personal necesario para apoyar los procedimientos de recuperación del compromiso.
- Políticas que exigen comprobar la revocación de claves (para minimizar el efecto de un compromiso).
- La supervisión de las operaciones de recodificación (para garantizar que se realicen todas las operaciones necesarias para todas las claves afectadas).
- Cualquier otro procedimiento de recuperación de compromisos.
- Una inspección física del equipo.

- Una identificación de toda la información que puede estar comprometida como resultado del incidente.
- Identificación de todas las firmas que pueden ser inválidas debido al compromiso de una clave de firma.
- La distribución de nuevo material de codificación, si es necesario.

6.3.6 Gestión de llaves

- Separados lógica y físicamente de los datos que protegen.
- Cifrado con una *clave de cifrado* independiente.
- Almacenado dentro de una aplicación de gestión de claves dedicada.
- Situado en un entorno físico y lógicamente separado e inaccesible para usuarios no autorizados.

6.3.7 Llave privada y pública

- La validez de los parámetros del dominio se garantizará antes de la generación del par de claves o la verificación y validación de una firma digital.
- Cada par de claves se asociará a los parámetros del dominio a partir del cual se generó el par de claves.
- Un par de claves solo se utiliza para generar y verificar firmas utilizando los parámetros del dominio asociados con ese par de claves.
- La clave privada se utiliza únicamente para la generación de la firma, como se especifica en esta norma y se mantiene en secreto. La clave pública solo se emplea para la verificación de la firma y puede hacerse pública.
- El firmante previsto debe tener la seguridad de estar en posesión de la clave privada antes o al mismo tiempo que la utiliza para generar una firma digital.
- Una clave privada debe estar protegida contra el acceso, la divulgación y la modificación no autorizados.
- Una clave pública debe estar protegida de modificaciones no autorizadas (lo que incluye la sustitución). Por ejemplo, los certificados de clave pública firmados por una AC pueden proporcionar esta protección.
- Un verificador debe tener la seguridad de que existe un vínculo entre la clave pública, sus parámetros de dominio asociados y el propietario del par de claves.

- Un verificador obtendrá las claves públicas de manera fiable (por ejemplo, a partir de un certificado firmado por una AC en la que confíe la entidad o directamente del firmante previsto o declarado, siempre que la organización sea de confianza para el verificador y pueda autenticarse como fuente de la información firmada que se verifica).
- Los verificadores deben estar seguros de que el firmante declarado es el propietario del par de claves y de que este propietario poseía la clave privada que se utilizó para generar la firma digital en el momento que se generó la firma (es decir, la clave privada que está asociada con la clave pública que se utiliza para verificar la firma digital).
- Un firmante y un verificador deben tener la garantía de la validez de la clave pública.

Capítulo 7. Trabajos para el futuro

Se establece la posibilidad de realizar una nueva versión del documento que contenga el mismo modelo de selección de algoritmos dirigido a algoritmos poscuánticos y longitudes de llaves establecidas para estos, además de otra información relevante para implementarlos en la computación del futuro. Desde ahora se debe pensar el mecanismo y las funciones que se deben de tomar para cambiar a la nueva protección criptográfica a partir de los nuevos cambios que esto implique para la organización o persona individual que lo requiera integrar en sus funciones diarias.

Glosario

Nota. Las definiciones se toman íntegramente de las publicaciones de NIST y FIPS usadas en la investigación.

Acuerdo de llave	Un procedimiento para establecer claves (por parejas) en el que el material de clave secreto se genera a partir de la información aportada por dos participantes, de modo que ninguna parte pueda predeterminar el valor del material de cifrado secreto independientemente de las contribuciones de la otra parte. Contrasta con el transporte de claves.
Algoritmo	Un proceso matemático especificado claramente para el cálculo; un conjunto de reglas que, si se siguen, dan un resultado prescrito.
Algoritmo de cifrado por bloques	Una familia de funciones y sus funciones inversas que están parametrizadas por claves criptográficas. Las funciones asignan cadenas de *bits* de una longitud fija a cadenas de *bits* de la misma longitud.
Aprobado	Aprobado por FIPS o recomendado por NIST. Un algoritmo o técnica que está: 1) Especificado en una recomendación FIPS o NIST. 2) Adoptada en una recomendación FIPS o NIST. 3) Especificada en una lista de funciones de seguridad aprobadas por el NIST.
Autenticación	Un proceso que garantiza el origen y la integridad de la información que se

	comunica o almacena o la identidad de una organización que interactúa con un sistema.
Autenticación integridad de los datos	El proceso de determinar la integridad de los datos, también llamado autenticación de la integridad o verificación de la integridad.
Autoridad certificadora (CA)	La entidad de una infraestructura de clave pública (PKI) que es responsable de emitir certificados y exigir el cumplimiento de una política PKI.
Bit	Un dígito binario que puede tener un valor de 1 o 0
Byte	Un grupo de 8 *bits*
Cadena de bits	Una secuencia ordenada de 0 y 1. El *bit* más a la izquierda es el más significativo de la cadena. El *bit* más a la derecha es el menos significativo de la cadena.
Certificado	Un conjunto de datos que identifica de forma exclusiva un par de claves y un propietario que está autorizado para utilizar el par de claves. El certificado contiene la clave pública del propietario y, posiblemente, otra información y está firmado digitalmente por una autoridad de certificación (es decir, una parte de confianza), vinculando la clave pública al propietario.
Compromiso	La divulgación, modificación, sustitución o utilización no autorizada de datos sensibles (por ejemplo, una clave secreta una clave privada o metadatos).

Confidencialidad	La propiedad de que la información sensible no se revele a entidades no autorizadas (es decir, se mantiene el secreto de la información clave).
Cripto periodo	El lapso durante el cual se autoriza el uso de una clave específica o en el que las claves de un determinado sistema pueden permanecer en vigor.
Criptografía	La disciplina que engloba los principios, medios y métodos para proporcionar seguridad a la información, lo que incluye la confidencialidad, integridad de los datos, autentificación de la fuente y no repudio.
Datos firmados	Los datos o mensajes sobre los que se ha calculado una firma digital calculada. Véase también “mensaje”.
Derivación de llave	El proceso por el cual el material de clave se deriva de una clave precompartida o un secreto compartido producido durante un esquema de acuerdo de claves junto con otra información.
Desencriptación	El proceso de cambiar el texto cifrado en texto plano utilizando un algoritmo criptográfico y una clave.
Digest	El resultado de una función *hash* criptográfica. Además, se denomina valor *hash*.
Entidad	Un individuo (persona), organización, dispositivo o proceso. Se utiliza indistintamente con “parte”.

Esquema	Conjunto de transformaciones especificadas sin ambigüedad que proporcionan un servicio (criptográfico) (por ejemplo, establecimiento de claves) cuando se ha implementado y mantenido adecuadamente. Un esquema es una construcción de nivel superior a una primitiva y de nivel inferior a un protocolo.
Establecimiento de llave	El proceso por el cual el material de clave se deriva de una clave precompartida o un secreto compartido producido durante una clave o un secreto compartidos producido durante un esquema de acuerdo de claves junto con otra información. Esquema de acuerdo de claves junto con otra información.
FIPS	Federal Information Processing Standard (estándar federal de procesamiento de información)
Firma digital	El resultado de una transformación criptográfica de datos que, cuando implementada correctamente, proporciona un mecanismo para verificar el origen, autenticación, integridad de los datos y no repudio del firmante.
Firma digital	El resultado de una transformación criptográfica de datos que, cuando implementada correctamente, proporciona los servicios de: 1. Autenticación de la fuente. 2. Integridad de los datos y

	3. Soporte para el no repudio del firmante.
Fuerza de seguridad	Un número asociado con la cantidad de trabajo (es decir, el número de operaciones) que se requiere para romper un algoritmo criptográfico o sistema. A veces, se denomina nivel de seguridad.
Función hash	Una función que asigna una cadena de *bits* de longitud arbitraria a una cadena de *bits* de longitud fija. Las funciones *hash* aprobadas se especifican en FIPS 180 y están diseñadas para satisfacer las siguientes propiedades: 1. (Unidireccional) Es computacionalmente inviable encontrar cualquier entrada que se corresponda con cualquier nueva salida preestablecida y 2. (Resistente a las colisiones) Es inviable desde el punto de vista informático encontrar dos entradas distintas que se correspondan con la misma salida
Garantía de la validez de la clave pública	Confianza en que la clave pública es aritméticamente correcta
Garantía de posesión	Confianza en que una entidad posee una clave privada y cualquier material de cifrado asociado.
Generación de la firma	El proceso de utilizar un algoritmo de firma digital y una clave privada para generar una firma digital sobre los datos.

Infraestructura de llave pública (PKI)	Un marco establecido para emitir, mantener y revocar certificados de clave pública.
Integridad de los datos	Propiedad por la que los datos no son alterados de forma no autorizada desde su creación, transmisión o almacenamiento.
Llave criptográfica	Un parámetro que se utiliza junto con un algoritmo criptográfico que determina su funcionamiento. Los ejemplos aplicables a esta norma incluyen: 1. El cálculo de una firma digital a partir de datos. 2. La verificación de una firma digital.
Llave privada	Una clave criptográfica que se utiliza con un algoritmo criptográfico asimétrico (de clave pública). En el caso de las firmas digitales, la clave privada está asociada de forma exclusiva al propietario y no se hace pública. La clave privada se usa para calcular una firma digital que puede verificarse utilizando la clave pública correspondiente.
Llave pública	Una clave criptográfica que se utiliza con un algoritmo criptográfico asimétrico (de clave pública) y está asociada con una clave privada. La clave pública está asociada con un propietario y puede hacerse pública. En el caso de las firmas digitales, la clave pública se usa para verificar una firma digital que se ha firmado con la correspondiente clave privada.

Mensaje	Una cadena de *bits* de cualquier longitud que es la entrada de una función SHA-3.
Mensaje digest	El resultado de aplicar una función *hash* a un mensaje. Además, se conoce como *valor hash*.
Módulo criptográfico	El conjunto de *hardware*, *software* o *firmware* que implementa funciones de seguridad aprobadas (incluidos los algoritmos criptográficos y generación de claves) y que está contenido en un límite criptográfico
NIST	National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología)
No repudio	Un servicio que se utiliza para garantizar la integridad y el origen de los datos, de manera que la integridad y el origen puedan verificarse y validarse por un tercero como originado por una entidad específica en posesión de la clave privada (es decir, el firmante).
Par de llaves	Una clave pública y su correspondiente clave privada.
Parámetros de dominio	Parámetros que se utilizan con algoritmos criptográficos que suelen ser comunes a un dominio de usuarios. Un par de claves criptográficas DSA o ECDSA se asocia con un conjunto específico de parámetros de dominio.
Parte	Un individuo (persona), organización, dispositivo o proceso. Se utiliza indistintamente con *entidad*.

Primitiva	Operación sencilla que se define para facilitar la implementación en *hardware* o en una subrutina de *software*
Propietario	El propietario de un par de claves es la entidad que está autorizada para utilizar la clave privada de un par de claves.
Pseudoaleatorio	Se indica que un proceso o los datos producidos por un proceso son pseudoaleatorios cuando el resultado es determinista, pero también efectivamente aleatorio mientras la acción interna del proceso esté oculta a la observación. En fines criptográficos, efectivamente, significa “entre los límites de la fuerza de seguridad prevista”.
SHA	Secure Hash Algorithm (algoritmo *hash* seguro)
SP	Special Publication (publicación especial)
Suscriptor	Una entidad que solicitó y recibió un certificado de una autoridad de certificación.
Texto cifrado	
Validación de la firma	La verificación (matemática) de la firma digital y la obtención de las garantías adecuadas (por ejemplo, la validez de la clave pública, la posesión de la privada, etc.).
Valor hash	Ver *mensaje digest*
Vector de inicialización (IV)	Un vector que se utiliza para definir el punto de partida de un proceso criptográfico

Verificación de la firma	El proceso de utilizar un algoritmo de firma digital y una clave pública para verificar una firma digital en los datos.

Acrónimos

Nota. Las definiciones se toman íntegramente de las publicaciones de NIST y FIPS usadas en la investigación.

AC	Autoridad certificadora
AES	Estándar de cifrado avanzado
AR	Autoridad de registro
CBC	Modo de encadenamiento de bloques de cifrado
CFB	Modo de retroalimentación del cifrado
CKMS	Sistema de gestión de llaves criptográficas
CTR	Modo contador
D	La longitud del compendio de una función *hash* o la longitud solicitada de la salida de un XOF, en *bits*.
DES	Estándar de cifrado de datos
DLC	Criptografía de logaritmos discretos, que se compone de criptografía de campo finito (FFC) y la criptografía de curva elíptica (ECC).
DH	Algoritmo Diffie-Hellman
DRGB	Generador de *bits* aleatorios determinístico
DSA	Algoritmo de firma digital
ECB	Modo de libro de códigos electrónico
ECC	Criptografía de curvas elípticas
ECDSA	Algoritmo de firma digital de curva elíptica
ECDSA	Algoritmo de firma digital de curva elíptica
FFC	Criptografía de campos finitos
GCM	Modo contador de Galois

HMAC	Código de autenticación de mensajes con clave *hash*
K^t	Valor constante para usarse para la iteración de t de la computación *hash*
(L, N)	El par asociado de parámetros de longitud para un par de claves DSA, donde L es la longitud de p y N es la longitud de q.
L(M)	Para una cadena de *bits* X, L(X) es la longitud de X en *bits*.
M	Número de *bits* en un bloque de mensaje
M	Mensaje que se computa con *hash*
N	1) Para RSA, el módulo; la longitud de *bits* de n se considera el tamaño de la clave. 2) En el caso de ECDSA, el orden del punto base de la curva elíptica; la longitud de *bits* de n se considera el tamaño de la clave.
MAC	Código de autentificación del mensaje
MQV	Algoritmo Menezes-Qu-Vanstone
OFB	Modo de retroalimentación de salida
P	1) Para DSA, uno de los parámetros del dominio DSA; un número primo que define el campo de Galois GF(p) y se usa como módulo en las operaciones de GF(p). 2) Para RSA, un factor primo del módulo n.
PKCS	Estándar de criptografía de llave pública
PKI	Infraestructura de llave pública

Q	1) Para DSA, uno de los parámetros del dominio DSA; un factor primo de p-1. 2) Para RSA, un factor primo del módulo n
RBG	Generador de *bits* aleatorios
RFC	Solicitud para comentario
RSA	Algoritmo desarrollado por Rivest, Shamir and Adleman
TCG	Grupo de computación de confianza
TDEA	Algoritmo de cifrado de datos triple
TLS	Seguridad de la capa de transporte

Referencias

CCN-CERT. (2022). *Defensa frente a las ciberamenazas*. https://www.ccn-cert.cni.es/

Dolendro Singh, L. y Manglem Singh, K. (2015). *Implementation of Text Encryption using Elliptic Curve Cryptography*. https://reader.elsevier.com/reader/sd/pii/S0898122104900181?token=A1E995C105D4A504D7FACBCECEF4654E39502BEC156819ADF81CF96B81DD4E5A7457D307482C2E9ABCD3A5D49E82AA16&originRegion=us-east-1&originCreation=20221030065549

IRTF. (2016). *Elliptic Curves for Security*. https://www.rfc-editor.org/rfc/pdfrfc/rfc7748.txt.pdf

IRTF. (2017). *Edwards-Curve Digital Signature Algorithm (EdDSA)*. https://www.rfc-editor.org/rfc/rfc8032

Kaspersky. (2022). *Index Alphabetical*. Https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf

Lap-Piu, L. y Kwok-Wo, W. (2003). *A Random Number Generator Based on Elliptic Curve Operations*. https://reader.elsevier.com/reader/sd/pii/S0898122104900181?token=A1E995C105D4A504D7FACBCECEF4654E39502BEC156819ADF81CF96B81DD4E5A7457D307482C2E9ABCD3A5D49E82AA16&originRegion=us-east-1&originCreation=20221030065549

NIST. (2001a). *Announcing the Advanced Encryption Standard (AES).* https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

NIST. (2001b). *Recommendation for Block 2001 Edition Cipher Modes of Operation Methods and Techniques*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

NIST. (2001c). *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf

NIST. (2007a). *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

NIST. (2007b). *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

NIST. (2008). *The Keyed-Hash Message Authentication Code (HMAC)*. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf

NIST. (2010a). *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf

NIST. (2010b). *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*. Https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf

NIST. (2010c). *Recommendation for Password-Based Key Derivation Part 1: Storage Applications*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90C.3pd.pdf

NIST. (2011). *Recommendation for Existing Application-Specific Key Derivation Functions*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf

NIST. (2012). *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*. Https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf

NIST. (2013). *A Framework for Designing Cryptographic Key Management Systems*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf

NIST. (2015a). *A Profile for U.S. Federal Cryptographic Key Management Systems*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-152.pdf

NIST. (2015b). *Efficient and Secure Elliptic Curve Cryptography Implementation of Curve P 256*. https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust

NIST. (2015c). *Recommendation for Key Management Part 3: Application-Specific Key Management Guidance*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf

NIST. (2015d). *Recommendation for Key-Derivation Methods in Key-Establishment Schemes*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf

NIST. (2015e). *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

NIST. (2015f). *Secure Hash Standard (SHS)*. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

NIST. (2015g). *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

NIST. (2016). *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-185.pdf

NIST. (2018a). *Recommendation for Key Establishment Using Symmetric Block Ciphers*. https://csrc.nist.gov/CSRC/media/Publications/sp/80071/draft/documents/sp800-71-draft.pdf

NIST. (2018b). *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/nist.sp.800-56Ar3.pdf

NIST. (2018c). *Recommendation for the Entropy Sources Used for Random Bit Generation*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf

NIST. (2019a). *Digital Signature Standard (DSS)*. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5-draft.pdf

NIST. (2019b). *Recommendation for Block Cipher Modes of Operation Methods for Format-Preserving Encryption*. Https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf

NIST. (2019c). *Recommendation for Key Management: Part 2 - Best Practices for Key Management Organizations*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt2r1.pdf

NIST. (2019d). *Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf

NIST. (2019e). *Recommendations for Discrete Logarithm-Based Cryptography: Elliptic Curve Domain Parameters*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-186-draft.pdf

NIST. (2019f). *Security requirements for cryptographic modules*. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

NIST. (2019g). *Transitioning the Use of Cryptographic Algorithms and Key Lengths*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

NIST. (2020a). *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175Br1.pdf

NIST. (2020b). *Public Comments Received on Draft NIST SP 800-186: Recommendations for Discrete Logarithm-Based Cryptography: Elliptic Curve Domain Parameters*. https://csrc.nist.gov/CSRC/media/Publications/sp/800-186/draft/documents/sp800-186-draft-comments-received.pdf

NIST. (2020c). *Recommendation for Cryptographic Key Generation*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf

NIST. (2020d). *Recommendation for Key Management: Part 1 - general*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

NIST. (2020e). *Recommendation for Stateful Hash-Based Signature Schemes*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf

NIST. (2021). *Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*. https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexa.pdf

NIST. (2022a). *CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140Cr1.pdf

NIST. (2022b). *CMVP Approved Sensitive Security Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759.*

NIST. (2022c). *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program*. https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf

NIST. (2022d). *Recommendation for Random Bit Generator (RBG) Constructions*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90C.3pd.pdf

OWASP. (2021). *¿Qué es el cifrado de datos? Definición y explicación*. https://cheatsheetseries.owasp.org/Glossary.html

Sealpath. (2020). *Protegiendo la información en sus tres estados*. https://www.sealpath.com/es/blog/tres_estados_info/

Apéndices

Apéndice A: Curvas recomendadas por NIST para el algoritmo ECDSA

Longitudes de bits de los campos subyacentes de las curvas recomendadas		
Longitud de bits de '*n*' (la llave)	**Campo primo**	**Campo binario**
224 – 255	Len(p) = 224	M = 233
256 – 383	Len(p) = 256	M = 283
384 – 511	Len(p) = 384	M = 409
≥ 512	Len(p) = 521	M = 571

Apéndice B: Propiedades de los algoritmos hash de la familia SHA-2 aprobadas

Algoritmo	**Tamaño de mensaje (bits)**	**Tamaño de bloque (bits)**	**Tamaño de palabra (bits)**	**Tamaño del mensaje Digest**
SHA-224	$< 2^{64}$	512	32	224
SHA-256	$< 2^{64}$	512	32	256
SHA-384	$< 2^{64}$	512	32	384
SHA-512	$< 2^{128}$	1024	64	512
SHA-512/224	$< 2^{128}$	1024	64	224
SHA-512/256	$< 2^{128}$	1024	64	256

Apéndice C: Fuerza de seguridad de las funciones SHA-2 y SHA-3 aprobadas.

Función	**Tamaño de salida**	**Fuerza de seguridad en bits**		
		Colisión	Preimagen	2nd Preimagen
SHA-224	224	112	224	Min(224, 256 – $L(M)$
SHA-512/224	224	112	224	224
SHA-256	256	128	256	256 – $L(M)$
SHA-512/256	256	128	256	256

SHA-384	384	192	384	384
SHA-512	512	256	512	512 – $L(M)$
SHA3-224	224	112	224	224
SHA3-256	256	128	256	256
SHA3-384	384	192	384	384
SHA3-512	512	256	512	512
SHAKE128	D	Min(d/2, 128)	≥ min(d,128)	Min(d, 128)
SHAKE256	D	Min(d/2, 256)	≥ min(d, 256)	Min(d, 256)