Protocolo Diffie-Hellman Usando la Curva Elíptica Para la Distribución de Llaves de un Criptosistema Simétrico.

Trabajo Terminal No.

Alumno: Miranda Sánchez Diego Alfonso.
Directores: Dr. Luna Benoso Benjamín, Dr. Víctor Manuel Silva García.
***email:** dmirandas1000@alumno.ipn.mx*

Resumen - En el presente trabajo, se implementó una mayor seguridad sobre comunicaciones basadas en curva elíptica utilizando el protocolo Diffie-Hellman como medio de distribución de llaves privadas de criptosistemas simétricos. Para lograr esto, los elementos utilizados fueron un canal de comunicacíon electrónico, un criptosistema asimétrico basado en criptografía de curva elíptica y finalmente se implementó el protocolo Diffie-Hellman para proveer una capa adicional de seguridad. La importancia del presente radica en mejorar la seguridad de las comunicaciones que utilizan curva elíptica, y sus aplicaciones contemplan las plataformas de comunicación y tecnologías de la información actuales.

Abreviaturas: Mod. (Módulo), Trad. (Traducción al español). I.e. (es decir), Ing. (Ingeniería). Sii (Sí y sólo sí).

Acrónimos: PDH (Protocolo Diffie-Hellman), CCE (Criptografía de Curva Elíptica), CE (Curva elíptica), CS (Criptosistema Simétrico), CA (Criptosistema Asimétrico), AA (Análisis del Algoritmo), IoT (Internet Of Things, Trad. Internet de las Cosas), TIC (Tecnologías de la información y la comunicación), SGSI (Sistema de Gestión de Seguridad de la información), ESCOM (Escuela Superior de Cómputo).

Palabras Clave – Aritmética Modular, Criptografía, Criptosistema Asimétrico, Curva Elíptica.

1. Introducción

En criptografía, el intercambio de llaves es un procedimiento para transmitir una clave, entre un transmisor y un receptor. El problema del intercambio seguro de información es que nadie pueda entenderla excepto por el transmisor y el receptor. El protocolo Diffie-Hellman del presente es implementado sobre una curva elíptica con 2^{256} puntos solución, ofreciendo gran seguridad y una solución ante esta problemática. Esta técnica, refuerza la ya existente distribución de llaves mediante criptografía de curva elíptica. Esto permite mejorar este tipo de criptosistema aplicando el protocolo Diffie-Hellman fungiendo como una capa de seguridad añadida.

Existen trabajos que se han realizado y que han aportado al mejoramiento de la seguridad en los sistemas criptográficos, como el de primitivas criptológicas que refuerzan la complejidad de las comunicaciones y el almacenamiento.[1]

Un estudio referente al presente, es el reforzamiento de autenticaciones en nubes públicas utilizando criptosistemas híbridos.[2]

Criptografía de curva elíptica: Un breve introductorio

Es importante describir la curva elíptica utilizada para entender el presente trabajo. La curva elíptica es una ecuación de tercer grado y puede ser y puede ser descrita sobre un intervalo continuo o discreto de numeros reales. Relativo a los esquemas de comunicación segura. Es un protocolo criptográfico asimétrico establecido sobre un grupo abeliano discreto. Es decir, para nuestro propósito la curva elíptica es implementda sobre el conjunto de números discretos. De forma general, la curva elíptica, que denotaremos como E, tiene la forma:

1. $y^2 \equiv x^3 + ax + b \; mod(p)$ donde a, b y $x \in \mathbb{R}$, también conocida como ecuación de Weierstrass.

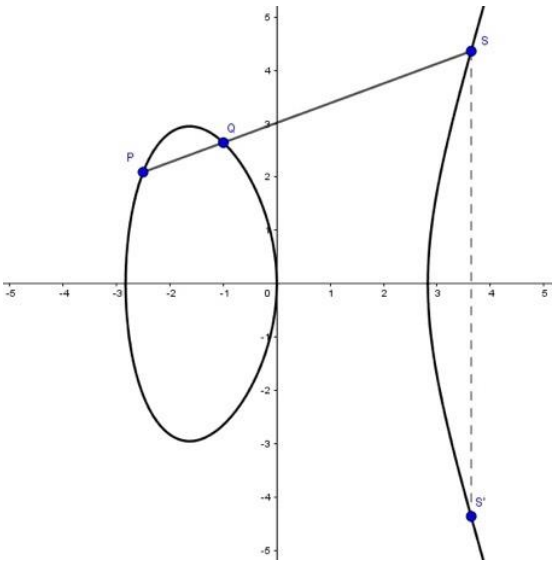


Figura 1: Gráfica de la Ecuación 1.

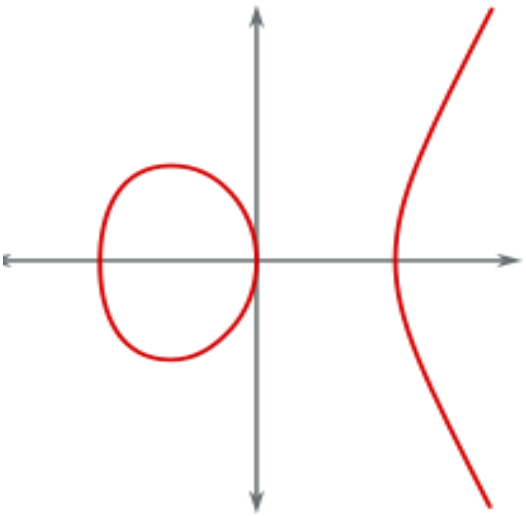


Figura 2: Gráfica de la Ecuación 2 con k=1.

Cabe mencionar que esta (ec. 1) es la forma general de la CE. Pero existen innumerables curvas elípticas. Para nuestro caso de implementación en el protocolo, usaremos la curva:

2. $y^2 \equiv x^3 - kx \, mod(p)$ donde k y $x \in \mathbb{R}$.

Esta curva seleccionada, tiene 3 raíces reales. Para cumplir con esta condición se debe probar que $4a^3 + 27b^2 \neq 0$. Cuando una curva elíptica cumple con esta condición, se le conoce como curva no singular.

Sea el punto P de la figura 1, un punto cuyas coordenadas (x_1, y_1), y las coordenadas del punto Q sean (x_2, y_2), entonces se pueden dar las siguientes tres combinatorias de eventos:

1. Que las abscisas $x_1 \neq x_2$.
2. Que se cumpla $x_1 = x_2$ y las ordenadas $y_1 = -y_2$.
3. Que las abscisas y las ordenadas sean iguales; i.e. $x_1 = x_2 \, y \, y_1 = y_2$.

En el primer caso, es evidente que los puntos son diferentes, caso de la figura 1. En esta situación la línea recta que pasa por los puntos P y Q pasa por la gráfica de la curva en el punto S. Entonces, se define la suma de P + Q como el punto S'. Esto implica que si S = (x_3, y_3), entonces S' = $(x_3, -y_3)$.

Entonces, basado en Geometría Analítica, se puede obtener la recta dados dos puntos (x_1, y_1) y (x_2, y_2). Una vez calculada esta línea recta, es posible calcular el punto (x_3, y_3) y por tanto a S'.

Se define la pendiente de la ecuación $y = \lambda x + \beta$ de la siguiente forma:

3. $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$

Y los puntos. x_3 y y_3 :

4. $x_3 = \lambda^2 - (x_1 + x_2)$.

5. $y_3 = \lambda(x_1 - x_3) - y_1$

Para el segundo caso, se cumple que Q es el inverso aditivo de P. Esto implica que $x_1 = x_2$ y que $y_1 = -y_2$. Para este caso la pendiente de la recta que pasa sobre los puntos forma un ángulo de $90°$ con respecto al eje de las abscisas. Es entonces cuando es evidente que esta pendiente es un valor no acotado, i.e. que tiende a ser ∞. Entonces concluímos que para este caso; si P es el inverso aditivo de Q entonces $(x_1, y_1) + (x_2, y_2) = \infty$. A su vez, también se cumple que para cualquier punto P = (x_n, y_n), P + ∞ = P. Definimos entonces a ∞ como el elemento nulo.

Para el tercer caso, la pendiente es obtenida mediante la ecuación

6. $\lambda = \frac{3x_1^2 + a}{2y_1}$.

Esto implica que los puntos solución x_3, y_3 son calculados de la forma

7. $x_3 = \alpha - 2x_1$

Siendo el cálculo de y_3 es igual al de la expresión 5.

Condicionantes específicas

Las condicionantes específicas para la curva que usaremos: $F_p : y^2 \equiv x^3 - kx \, mod(p)$ donde k y $x \in \mathbb{R}$, son:

8. $4((-k)^3) \not\equiv 0 \, mod \, p$

9. $\#E(F_p) \not\equiv 1 \, mod \, p$

10. $\#E(F_p) \neq p$

Donde $\#E(F_p)$ denota el número de soluciones de F_p.

Sistemas similares que se han desarrollado son:

1.-GPG (GNU Privacy Guard).[4] Refuerza permitiendo firmas, además de un extenso catálogo de bibliotecas.
2.-Proyecto de Investigación - Cryptographic Primitives Enforcing Communication and Storage Complexity.
3.-Enforcing Confidentiality and Authentication over Public Cloud Using Hybrid Cryptosystems – De la conferencia internacional en tecnologías de comunicación inteligentes y el IoT.

Tabla comparativa entre softwares/investigaciones:

Software/ Característica	Doble Sistema asimétrico	Primitivas nuevas	API extensa	Trabajo en la nube	Asimétrico	Simétrico	Híbrido
A)			•				•
B)		•					
C)				•			•
D)	•				•		

A) GPG.
B) Primitivas Criptográficas Reforzando las Comunicaciones y la Complejidad de Almacenamiento.
C) Reforzando la Confidencialidad y la Autenticación sobre nubes públicas usando criptosistemas híbridos.
D) Protocolo Diffie-Hellman usando la curva elíptica para la distribución de llaves de un criptosistema simétrico.

2. Objetivo

Implementar un sistema de subrutinas en una arquitectura de capas basada en el protocolo Diffie Hellman como capa superior y en curva elíptica como capa inferior o sistema base, para reforzar la seguridad del intercambio de llaves; además, de información sensible en general, permitiendo una elevada seguridad frente a los ataques enfocados a interceptación de datos, en específico los ataques de apropiación de información en procesos de comunicación de aplicaciones y servicios, mejorando la seguridad en estos y demostrando su eficacia comparado al método de distribución de llaves usando curva elíptica simple, llámense curvas elípticas basadas en la ecuación de Weiestrass, y como resultado obtener una solución fiable ante el problema de las comunicaciones poco confiables sobre canales de comunicación públicos, originado por la naturaleza no segura de los mismos, teniendo aplicaciones directas en sectores como lo son el gubernamental, el militar y el empresarial.

3. Justificación

El porcentaje de organizaciones afectadas por un ataque de ciber seguridad se ha incrementado durante los previos 3 años de un 78% a un 80.7%. [5] Ataques que contemplan un abanico de diversas naturalezas, desde malware, *phishing*, *abuso de credenciales*, hasta ataques de día cero. Esto tiene graves implicaciones y repercusiones en distintos ámbitos como lo son las telecomunicaciones, el cuidado de la salud, la industria de la fabricación, los procesos automatizados, el sector gubernamental, los sistemas bancarios, de pérdidas económicas y en consecuencia de perjuicio a personas físicas y morales. Es entonces cuando de nuevo afrontamos una problemática a nivel mundial. Esta se debe si bien no erradicar por su naturaleza variable e incontrolable debido a la incapacidad de las organizaciones y profesionales de las TIC de controlar a todas las instancias que representan a una ciber amenaza a nivel global, sí se debe mantener bajo una cota necesaria, y esta cota debería ser decreciente con respecto al tiempo siendo capaz de ser observable estadísticamente.

Uno de los ataques criptológicos más conocidos son los ataques de criptoanálisis y/o interceptación de canal para descifrado de información sensible, permitiendo el abuso de credenciales. Para nuestro caso de estudio, el presente propone un método de mejora a los sitemas clásicos de criptografía de curva elíptica, así haciendo frente a los ataques de lógica enfocada a vulnerabilidades de comunicación en aplicaciones y servicios, permitiendo una elevada seguridad en comunicaciones electrónicas y de este modo, ofreciendo una solución fiable ante la interceptación de información por entidades no autorizadas. El protocolo aquí propuesto ofrece un gran beneficio, el cual es, un incremento de la seguridad en las comunicaciones realizadas mediante canales de información inseguros. Para lograr esto, se propone un novedoso sistema de asimetría doble en capas, contribuyendo así al desarrollo tecnológico y a los SGSI mediante resultados útiles y medibles como lo son la reducción en la probabilidad del descifrado exitoso de información interceptada, repercutiendo en inmediatos usuarios potenciales beneficiados, por mencionar algunos, el sector gubernamental, militar y empresarial. La complejidad del presente a nivel ingeniería radica en la comprensión teórica sobre la matemática aplicada a la criptografía que subyace al protocolo, la capacidad que el sistema tiene ante una amenaza real y la confiabilidad ante esta, y de una implementación ordenada y estandarizada del producto.

Para ejemplificar, el presente es funcional evitando ataques de interceptación de información como Man In The Middle. Debemos señalar, que una de las principales vulnerabilidades dentro de una empresa no son sus métodos de autenticación y/o cifrado. Las más grandes barreras para mantener una seguridad óptima en un sector empresarial son la carencia de personal de seguridad de las TIC con las suficientes habilidades y la falta de conciencia en los empleados acerca de conceptos como la seguridad informática y a la ingeniería social. Uno de los problemas enlistados dentro de las principales preocupaciones de las empresas relativas a la seguridad de su entorno, es es el abuso de credenciales, las cuales pueden ser obtenidas de forma ilegítima utilizando diversas técnicas, como la interceptación de canal o un tipo de ingeniería social en la que el atacante intenta obtener información sensible de usuarios haciéndose pasar por una entidad de confianza, esta es la definición de *phishing*, (CompTIA Security+ Exam SY0-501[6]).

Para evitar este tipo de ataques es fundamental fomentar la conciencia sobre hermetismo y otras políticas de seguridad necesarias en la empresa. A su vez, para que este protocolo sea funcional ante técnicas elaboradas y novedosas de ingeniería social, es vital establecer como normativa de la empresa en sus políticas, que la

comunicación de información sensible sea sólo establecidada usando el protocolo, para evitar interceptación de canal o phishing, preocupación que enlista el segundo lugar en el *gráfico 1.*

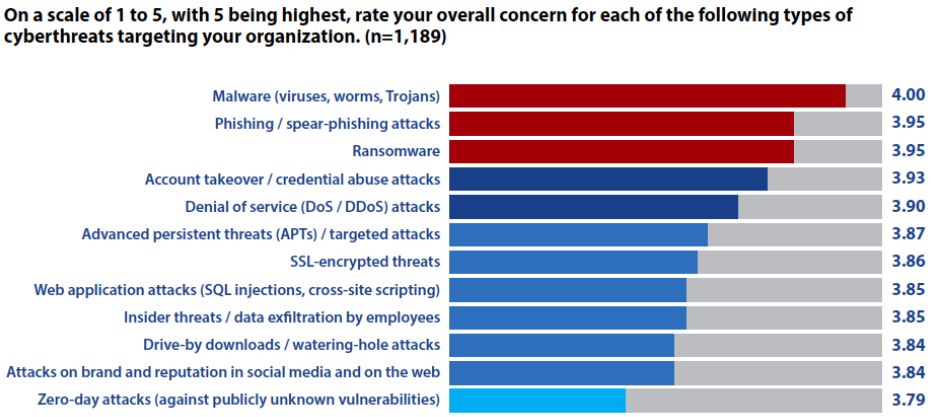


Gráfico 1: Encuesta sobre amenazas empresariales preocupantes de Cryber Edge Group 2020 (ref. 5).

Tanto la preocupación por el phishing como el robo de cuentas y credenciales se observa en la sección 2 del reporte de ciber amenzas de Cyber Edge Group de 2020 la cual es una gran firma especializada en investigación de las necesidades de los proveedores de servicios y tecnologías. En el gráfico de preocupaciones sobre ciber amenzas (gráfico 1) observamos que la apropiación indebida de información sensible ocupa un alarmante cuarto lugar en la lista con un promedio 3.93 puntos de 5 habiendo recibido las respuestas de 1200 tomadores de decisiones de seguridad certificados, y todas las organizaciones teniendo más de 500 empleados como informa el reporte (pág: 3).

Dadas estas circunstancias, la necesidad de implementar un sistema de distribución de llaves e información sensible como contraseñas y nombres de usuarios para evitar su apropiación indebida, y que ofrezca una mejor seguridad a los métodos tradicionales es real y siempre constante. Es fundamental recalcar que el protocolo presentado previene el abuso de información sensible por la naturaleza de su mecanismo. Se propone un sistema de asimetría doble para cifrar la información sensible que viaja por los nodos de una red, evitando su entendimiento. Un evaluador profesional de riesgos potenciales conoce que la interceptación de información no autorizada que se transmite por un canal electrónico inseguro, siempre es un riesgo inminente.

Este trabajo presenta un novedoso sistema de dos capas de cifrado y distribución asimétrica, actuando como capa subyacente la criptografía de curva elíptica y como superior el protocolo Diffie-Hellman.

Los usuarios potenciales abarcan un amplio espectro de sectores de la sociedad. Los directamente beneficiados, por mencionar algunos, son el sector empresarial, la industria militar, y sector de telecomunicaciones.

Cabe mencionar, que este trabajo mejora el ya existente trabajo existente sobre criptografía de curva elíptica, propuesta de forma independiente por Victor Miller y Neal Koblitz y en 1985 y 1987.[7][8]

La complejidad de esta implementación contempla múltiples áreas del conocimiento, como primera mención el profundo conocimiento de las áreas de criptología asociadas, como la curva elíptica, el protocolo Diffie-Hellman, el problema del logaritmo discreto. Todos estos conocimientos poco comunes, requieren tiempo y práctica para su comprensión. Se precisa tener un nivel elevado en el manejo de la aritmética modular, cálculo y números primos, así como un nivel competente para diseñar y programar algoritmos, y al mismo tiempo el conocimiento de metodologías de desarrollo de software. La programación orientada a objetos y el conocimiento del lenguaje de programación serán necesarios para la buena organización, y los conocimientos de electrónica para la correcta implementación y evitar vulnerabilidades asociadas al hardware. El análisis y diseño orientado a objetos y la ingeniería de software para una implementación ordenada. El conocimiento de redes para comprender el funcionamiento de los canales de comunicación. Se precisa de 1440 horas mínimas para la culminación de este proyecto, es decir hasta la evaluación de TT2 en noviembre-diciembre.

4. Productos o resultados esperados

El protocolo funciona como un sistema de capas hacia arriba, en el cual la capa inferior recibe una entrada, cada capa entrega un conjunto de información, y el orden del proceso es ascendente, comenzando por la entrada A) como se muestra en el diagrama a):

Etapa	**Esquemas generales de cifrado**
E)Salida	**x**
D)Capa superior o capa 2.	**Protocolo Diffie-Hellman** **Tx** **A** **21)a** **22)a*α=P_A** **23)a*P_b=P** **24)a*b*α=P** **25)k_1*α=(x_0,y_0)** **26)y_0* l mod(p)≡ l`** **27)$y_1$=$k_2$\*$P_A$** **28)$y_2$=($x_0$,$y_0$) + $k_2$\*P** **Medio Público** **p,q,$\alpha$** **$P_A$** → **$P_b$** ← **l`,y_1,y_2** → **Rx** **B** **22)b** **23)b*α=P_b** **24)b*P_a=P** **25)b*a*α=P** **26)y_2-b*y_1=(x_0,y_0)** **27)(x_0,y_0)+k_2*P-k_2*P_A** **28)(x_0,y_0)+k_2*a*b*α=** **29)b*k_2*α = (x_0, y_0)** **30)y_0^{-1}mod(p) ≡** **y_0^{-1}*y_0*l mod(p) ≡ l**
C)Salida de la capa inferior	**α,x,a,b,k_1,k_2,p,q,k=l**
B)Capa inferior o capa 1	**Curva Elípitca** **Tx** **A** **1)M=msg** **2)k=bin(x)** **3)m_A=Apriv.key** **4). β_A=m_A*α** **5)L, 1<L<q-1** **6)L*α=(x_0,y_0)** **7)y_1=x*α** **8)y_2=L*α+x*β** **7)n^*=y_0*xmod(p)** **8)n^*=x_0*xmod(p)** **9)e_{AESx}(M) = M*** **Medio Público** **p,q,α,β** **y_1,y_2,M^*,n^*** → **Rx** **B** **10)m_b=Bpriv.key** **11)β_b=m_b*α** **12) L*α=(x_0,y_0) =** **y_2-m*y_1** **13)$n^*(y_0)^{-1}$ mod(p)** **14)y_0*x*$(y_0)^{-1}$mod(p)** **15)x=x** **16)usando x_0:** **17)$n^*(x_0)^{-1}$ mod(p)** **18)x_0*x*$(x_0)^{-1}$mod(p)** **19)x=x** **20) $d_{AESx}(M^*)$ = M**
A)Entrada	**x,p,q,m_A,m_b,k,M,L,a,b**

Diagrama a): Esquema algorítmico/matemático para mostrar el funcionamiento, estructura de dos capas y flujo hacia arriba del protocolo.

Explicación del diagrama a)

En este diagrama por capas es posible observar el comportamiento del protocolo. Se tiene como instancia de entrada al algoritmo el conjunto I, a su vez, se tiene el problema de la distribución de información de forma segura, problema que definiremos como P, y puede ser visto como una función $P: I \rightarrow S$, siendo I el conjunto de instancias de entrada (datos sensibles) y S un conjunto de soluciones. La instancia I que se contempla para el ejemplar, es un conjunto de elementos de naturaleza numérica, la llave del sistema simétrico x o en general cualquier información representable como una cadena numérica binaria (base 2), dos números primos $p\ y\ q$, dos números pseudo aleatorios m_A y m_B los cuales fungirán como llaves privadas del emisor y transmisor, un número k que es la representación binaria de x, un M el cual representa un mensaje compuesto por cadenas de texto, para nuestro caso de estudio este es meramente ilustrativo, ya que el sistema es orientado a la distribución de llaves asimétrica. Un número L acotado por 1 y $q-1$ no inclusive, es decir: $1 < L < q-1$ y un a y b pseudo aleatorios que sirven en la segunda capa para construír las llaves públicas. Estos son procesados por las operaciones modulares indicadas en el diagrama etapa 1 para obtener una salida que cumple con las características de un sistema LTI (Trad. Lineal e invariante en tiempo). En esta salida, tenemos el elemento α, el cual es elemento generador de soluciones para la curva elíptica. K_1 y k_2 son provistos por la capa inferior, elementos necesarios para el cifrado en la capa superior. Los p y q se transmiten intactos. Renombramos k por l. Estos elementos son procesados por la capa superior, aplicando las operaciones aritméticas explícitas en el diagrama, también llamado esquemas generales de cifrado. Finalmente, en la salida obtenemos la clave del sistema simétrico, el entero x, el cual a su vez tiene una representación binaria, y que puede representar cualquier tipo de información, dependiendo de los acuerdos.

Como producto final, también se anexa código, documentación técnica y manual de usuario.

5. Metodología

Es fundamental establecer normativas, metodologías, y modelos de desarrollo de software para el correcto y organizado desarrollo de un proyecto. Cuando un software cumple su función, es a causal de que sus subrutinas y los elementos que lo confoman, han sido implementados de forma enfocada y ordenada. Esto tiene un impacto directo en la facilidad para editar o incrementar sus módulos y el nivel de satisfacción de los usuarios, lo que implica una repercusión económica y de desarrollo tecnológico importante. Para que un software sea correctamente desarrollado, es necesario un enfoque de ingeniería.

Para el presente, se utilizarán dos enfoques ingenieriles de desarrollo. El primero, fungiendo como capa subyacente para el desarrollo de este proyecto será el estándar **ISO 27001.** La aplicación de este esándar en este proyecto permite evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros.[9] La meta intermedia es que el protocolo se encuentre implementado y que se observe sea estable, repercutiendo en su confiabilidad y seguridad. Se deberán contemplar las distintas etapas del estandar ISO 27001 sobre el protocolo, para que este cumpla con sus normativas:

Planificación

- Definir la política de seguridad.
- Establecer el alcance del SGSI.
- Realizar el análisis de riesgo.
- Seleccionar los controles.
- Definir competencias.
- Establecer un mapa de procesos.
- Definir autoridades y responsabilidades.

Hacer

- Implantar el plan de gestión de riesgos.

- Implantar el SGSI.
- Implantar los controles.

Controlar

- Revisar internamente el SGSI.
- Realizar auditorías internas del SGSI.
- Poner en marcha indicadores y métricas.
- Hacer una revisión por parte de la Dirección.

Actuar

- Adoptar acciones correctivas.
- Adoptar acciones de mejora.

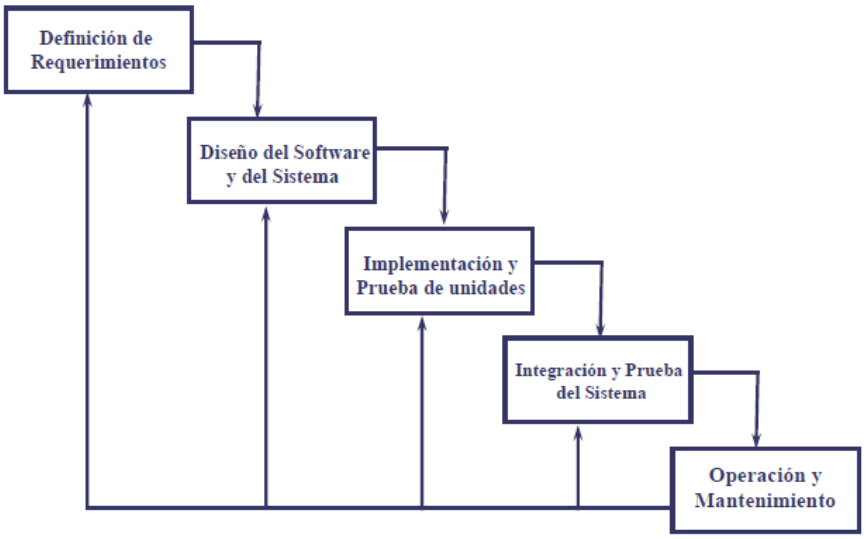
Para el enfoque de desarrollo del sotfware, se utilizará la *metodología en cascada*. En este modelo, el producto sufre una evolución o crecimiento conforme a una secuenica de pasos ordenados en forma lineal, permitiendo iteraciones al estado anterior.[10] El número de etapas puede variar, pero en general suelen ser (pero no estrictamente ni limitadas a):

- Análisis de requisitos del sistema.
- Análisis de requisitos del software.
- Diseño preliminar.
- Diseño detallado.
- Codificación y pruebas.
- Explotación (u operación) y mantenimiento.

Las principales características de este modelo son:

- Cada fase empieza cuando se ha terminado la anterior.
- Para pasar a la fase posterior es necesario haber logrado los objetivos de la previa.
- Es útil como control de fechas de entregas.
- Al final de cada fase el personal técnico y los usuarios tienen la oportunidad de revisar el progreso del proyecto.

En el siguiente diagrama se puede observar una aproximación a este modelo, la cual será utilizada para el desarrollo del presente:



6. Cronograma

CRONOGRAMA Nombre del alumno: Miranda Sánchez Diego Alfonso TT No:

Título del TT: Protocolo Diffie-Hellman usando la curva elíptica para la distribución de llaves de un criptosistema simétrico.

Actividad/Mes	ENE/22	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
Definición de requerimientos												
Diseño del software y del sistema												
Implementación												
Integración y pruebas del sistema												
Evaluación de TT1												
Operación y mantenimiento												
Implementación de módulos adicionales												
Implementación de documentación ISO												
Manual de usuario												
Documetación técnica												
Evaluación de TT2												

7. Referencias

[1]P. Golle, S. Jarecki and I. Mironov, ”Cryptographic Primitives Enforcing Communication and Storage Complexity”, in Lecture Notes In Computer Science Conference, 2002.

[2]N. Thillaiarasu, S. Chenthur Pandian, G. Naveen Balaji, A. Divya, and G. Divya Prabha, “Enforcing Confidentiality and Authentication over Public Cloud Using Hybrid Cryptosystems”, SNS College of Engineering, Coimbatore, India, 10.1007/978-3-030-03146-6_175, 2019.

[3]V. Silva, R. Flores, C. Rentería, B. Luna, J. Chimal, “IMAGE CIPHER APPLICATIONS USING ELLIPTICAL CURVE AND CHAOS”, *Int. J. Appl. Math. Comput. Sci.*, Vol. 30, No. 2, pp. 377–391, 2020.

[4]M. Copeland, J. Grahn and D. Wheeler. The GNU Privacy Handbook. USA. Free Software Foundation, 1999.

[5]Cyber Edge Group. “2020 Cyberthreat Defense Report”, USA, 2020.

[6]A. Conklin, G. White. CompTIA Security+ Esam SY0-501 guide, New York: McGraw-Hill, 2018.

[7]V. Miller, "Use Of Elliptic Curves In Cryptography", Exploratory Computer Science, IBM Research, Yorktown Heights. 1985.

[8]N. Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation Vol 48, USA, pp. 203-209, 1987.

[9] ISOTools Excellence Org, “La norma ISO 27001: Aspectos claves de su diseño e implantación”. Madrid, 2018.

[10] Z. Cataldi, F. Lage, R. Pessacq y R. García, “INGENIERIA DE SOFTWARE EDUCATIVO”, Laboratorio de Sistemas Operativos y Bases de Datos. Departamento de Computación. Facultad de Ingeniería UBA, pp. 2-3, 2002.

8. Alumnos y Directores

CARÁCTER: Confidencial
FUNDAMENTO LEGAL: Artículo 11 Fracc. V y Artículos 108, 113 y 117 de la Ley Federal de Transparencia y Acceso a la Información Pública.
PARTES CONFIDENCIALES: Número de boleta y teléfono.

Diego Alfonso Miranda Sánchez.- Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta 2014630322,
Tel. 5617449995, alfonso_miranda@outlook.com.

Firma: ACUSE DE RECIBIDO

Dr. Benjamín Luna Benoso. Licenciatura en Física y Matemáticas por la ESFM, maestría y doctorado en ciencias de la computación por el CIC. Profesor e investigador en la ESCOM. Áreas de interés: reconocimiento de patrones, autómatas celulares, criptografía. Email: blunab@ipn.mx.

Firma: ACUSE DE RECIBIDO

Dr. Silva García Victor Manuel. Dr. en Ciencias de la Computación del CIC IPN (2007), M. en C. En Estadística y Cálculo del Colegio de Posgrado de Chapingo (1981), Lic. En Física y Matemáticas de ESFM IPN (1974), Profesor de ESCOM (Departamento de Posgrado) y de CIDETEC IPN (2005), miembro del Sistema Nacional de Investigadores. Áreas de Interés: Criptografía y Redes. Tel: 5532031026, email vsilvag@ipn.mx.

Firma: ACUSE DE RECIBIDO