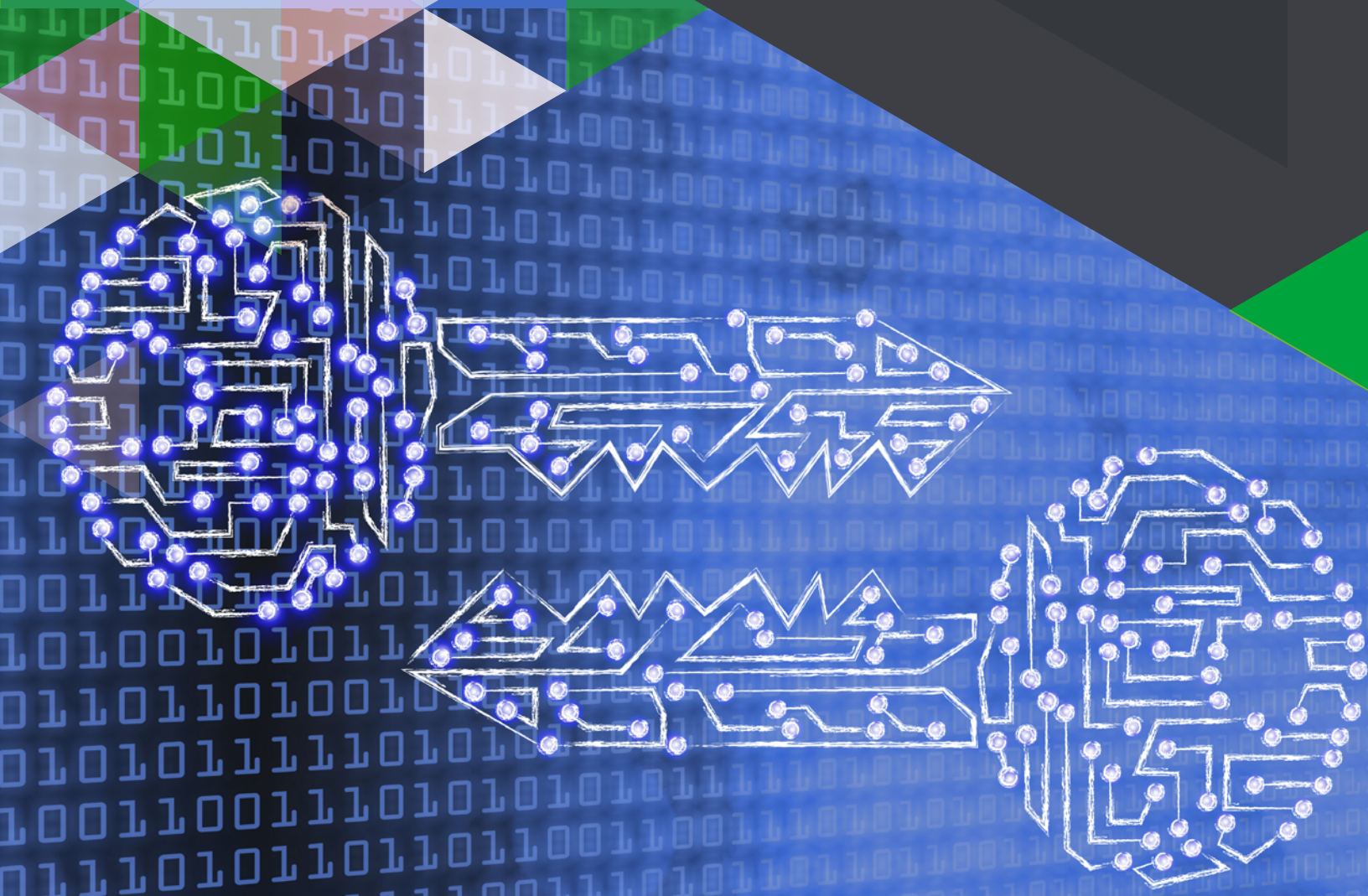
FUNDAMENTOS DE SEGURIDAD INFORMÁTICA

Ricardo López

EJE 2

Analicemos la situación



AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED ILUMNO

Fuente: Shutterstock/509910508

ÍNDICE

INTRODUCCIÓN

¿Cuál o cuáles procesos permiten mitigar los riesgos de seguridad a los que está expuesta la información?

Los beneficios de implementar una **metodología** para un sistema de seguridad informática radica en minimizar los riesgos, mitigar eventuales incidentes de seguridad y generar un ambiente de tranquilidad y confianza tanto a clientes internos como a clientes externos.

En este segundo eje del conocimiento se abarcará lo relacionado con el ciclo de mejora continua **PHVA** (PDCA por sus siglas en inglés), aplicado a los sistemas de gestión de seguridad Informática.

Se trabajará en las diferentes fases para integrar, implementar, verificar y sostener el sistema de seguridad en cualquier organización o entidad, generando procesos constantes de revisión y mejora.

El marco metodológico de este segundo eje es teórico–práctico, donde el estudiante a partir de los conceptos, generará análisis, implementará soluciones y propondrá nuevas alternativas de mejora.

Para el desarrollo de este eje nos apoyamos en video cápsulas, video relatos, lecturas complementarias, talleres, entre otros recursos de aprendizaje, para afianzar el conocimiento.

Metodología

Vista como un conjunto de procesos o procedimientos.

PHVA

Ciclo de mejora continua PHVA (Planear, Hacer, Verificar, Actuar).

Introducción a la seguridad informática

La seguridad informática ha sido un tema de interés desde el desarrollo del lenguaje, la necesidad de ocultar la información o volverla ilegible para las demás personas ha obligado a desarrollar métodos que permitan ocultarla, a estos métodos o técnicas se les denomina criptografía.

Debido al desarrollo y evolución de las técnicas criptográficas, se han dividido en dos grandes grupos, un primer grupo denominado criptografía clásica y un segundo grupo denominada criptografía moderna.

Ilegible
Hace referencia a lo confuso o no entendible.

Técnicas criptográficas
Son mecanismos y/o técnicas de cifrar la información.

Lectura recomendada

Los invito a realizar la lectura Criptografía para principiantes, la cual nos dará una primera visión de la importancia de la criptografía y las técnicas utilizadas para ocultar la información.

Criptografía para principiantes.

José de Jesús Ángel Ángel

Criptografía clásica

La criptografía clásica está compuesta por técnicas criptográficas desarrolladas en épocas antiguas utilizadas para ocultar o cifrar la información y/o mensajes que debían ser compartidos entre las diferentes personas y que por su grado de privacidad no podían ser divulgados públicamente.

Privacidad
Hace referencia a información sensible secreta, no divulgable

Las técnicas criptográficas más destacadas en esta etapa fueron la sustitución y la transposición.

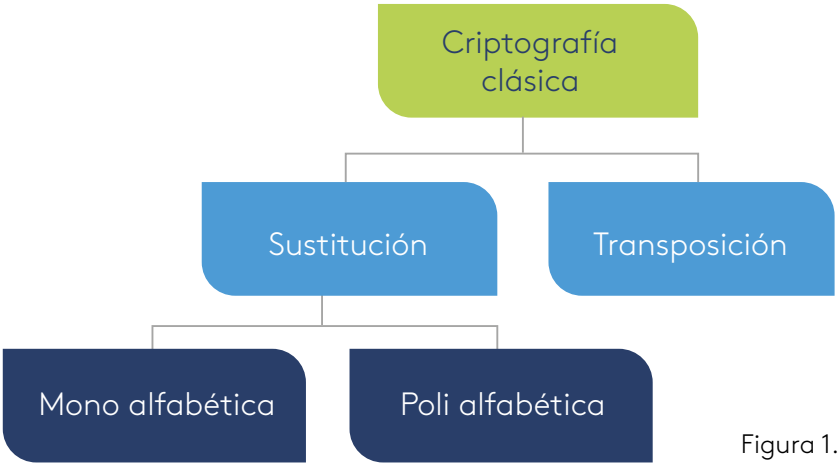


Figura 1. Criptografía clásica
Fuente: propia

Criptografía clásica por sustitución

La sustitución consistía en cambiar un grafo por otro, es decir, cambiar un carácter por otro, dependiendo de una llave o clave de cifrado.

La técnica más popular de cifrado por sustitución fue el denominado cifrado *César* llamado así por el emperador Romano Cayo Julio César, a quien se le atribuye su invención, esta técnica consistía en desplazar 3 posiciones del elemento original.

Ejemplo

Texto Original: GAFA DE ALEJA

Texto original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Equivalencia corrido 3 posiciones	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Tabla 1. Tabla de equivalencias
Fuente: propia

Cambiando carácter por carácter del texto plano, con la ayuda de la tabla de equivalencias se obtiene el texto encriptado, en el ejemplo anterior, tenemos que a la letra G del texto plano le corresponde la letra J, a la letra A le corresponde la letra D, a la letra F del texto plano le corresponde la letra I, y así sucesivamente hasta completar el mensaje, obteniendo el siguiente texto:

Texto encriptado: JDID GH DOHMD

El cifrado César es de muy bajo nivel de seguridad ya que un cripto-analista con facilidad podría descifrarlo sin necesidad de conocer la clave o llave, pues si nos fijamos en el ejemplo anterior, al carácter A siempre le corresponde el carácter D, al carácter E le corresponde el carácter H y así para cada símbolo.

Seguridad
Visto como ausencia de peligro o riesgo.

Si analizamos, cada idioma tiene una serie de símbolos o caracteres que se repiten con mayor frecuencia, en el idioma español son los caracteres A y E, sabiendo esto, podemos buscar los caracteres que más se repiten en el criptograma y los cambiamos por A y/o E y será un gran inicio para poder obtener el texto plano. A este tipo de cifrado se le denomina sustitución "mono alfabética".

Ante la facilidad de descifrar un algoritmo de sustitución mono alfabético se desarrollaron algoritmos poli alfabéticos, es decir, algoritmos en los cuales no hay una correspondencia repetitiva entre los caracteres, sino que, depende de una llave o clave.

Vigenère

Blaise de Vigenère a quien se le atribuye el cifrado poli alfabético

El algoritmo más popular de cifrado por sustitución poli alfabético es el cifrado de Vigenère, que consiste en una matriz que contiene todos los caracteres que forman el mensaje y una clave o llave que se relaciona directamente con el mensaje, dando como resultado, la intersección de la columna del carácter del texto plano con la fila del carácter de la llave o clave.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

Figura 2 Cifrado de Vigenère
Fuente: propia

Ejemplo

Texto plano: FUNDACION UNIVERSITARIA DEL AREA ANDINA

Clave: TILDE

Utilizando el cifrado de Vigenère obtenemos, el siguiente texto encriptado:

Texto plano	F	U	N	D	A	C	I	O	N	U	N	I	V	E	R	S	I	T	A	R	I	A	D	E	L	A	R	E	A	A	N	D	I	N	A
Llave o clave	T	I	L	D	E	T	I	L	D	E	T	I	L	D	E	T	I	L	D	E	T	I	L	D	E	T	I	L	D	E	T	I	L	D	E
Texto encriptado	Y	C	X	G	E	V	P	Z	P	Y	G	P	G	H	V	M	P	E	D	V	B	I	Ñ	H	O	T	Z	O	D	E	G	L	S	P	E

Tabla 2. Texto, clave y criptograma
Fuente: propia

Al analizar el resultado obtenido de encriptar un texto por medio de la matriz de Vigenère con una llave o clave, en este caso la palabra tilde, se observa que aparecen unas letras o caracteres que se repiten con mayor frecuencia, para nuestro ejemplo la P, G, V entre otras.

Si comparamos con el texto plano observamos que la primera G del texto encriptado corresponde a D, la segunda G corresponde a N, la tercera G corresponde a V, es decir cambia la correspondencia o equivalencia.

Ahora bien, si tomamos las "A" del texto plano y observamos los valores que toma cada una de estas en el texto encriptado tendremos que, A toma los valores de E, D, I, T. haciendo más complejo de descifrar este texto.

Video

Aunque el cifrado de *Vigenère* ha sufrido muchas variaciones se mantiene la matriz y la metodología de encriptación. Para una mejor comprensión del tema los invito a ver un ejemplo en el siguiente video relato.

Cifrado de Vigenère

https://drive.google.com/drive/folders/0B60bhF38XjruUmFLbzNEX2NqR2c

Video

Ahora, con el fin de complementar el aprendizaje de este interesante tema revise la video cápsula "Historia de la criptografía" la cual nos desarrolla un recorrido histórico sobre uno de los elementos fundamentales de la seguridad informática "la criptografía".

"Historia de la criptografía"

https://www.youtube.com/watch?v=a99Qorfotv4

Criptografía clásica por transposición

Figura 3. Escitala Espartana
Fuente: https://es.wikipedia.org/wiki/Esc%C3%ADtala

La transposición consiste en encriptar la información con los mismos caracteres del mensaje original, cambiándose de posición mediante un algoritmo, llave o clave.

La criptografía clásica de transposición se ha utilizado desde tiempos remotos, ejemplo de esto es la "*Escitala*", técnica utilizada por los espartanos (siglo VII a. C) que consistía en utilizar un trozo de madera de determinado grosor en el cual se enrollaba una cinta en forma de espiral y se escribía el mensaje longitudinalmente, una vez escrito el mensaje se desenrollaba y se enviaba al receptor o destinatario del mensaje, de tal forma que solo podía leer el mensaje quien tuviese un trozo de madera del mismo grosor el cual era la llave o clave.

Transposición
Cambiar de posición.

Ejemplo

La transposición a primera vista puede parecer un sistema simple de criptografía

Texto plano	FUNDACION UNIVERSITARIA DEL AREA ANDINA
Algoritmo, clave o llave	Vocales primero luego consonantes
Texto encriptado	UAIOUIEIAIAEAEAAIAFNDBNN-VRSTRDLRNDN

Pero la transposición se puede complejizar con una llave numérica que permita generar una matriz denominada bloques del tamaño de la llave.

Texto plano	FUNDACION UNIVERSITARIA DEL AREA ANDINA
Algoritmo, clave o llave	5
Texto encriptado	FCNSIANUIIIARDNOVTDEID-NEAEANAURRLAA

Veamos cómo se obtuvo el texto encriptado:

Como la llave es 5, creamos una matriz de 5 columnas y escribimos el mensaje de forma horizontal colocando en cada casilla una letra del mensaje.

El criptograma resultante se obtendrá escribiendo el texto por columnas, en caso de que, sobre alguna casilla, se debe llenar con un símbolo poco utilizado (Z, X, #, $,&,?,¿, entre otros), entre menos evidente sea el símbolo más complejo será el criptograma.

F	U	N	D	A
C	I	O	N	U
N	I	V	E	R
S	I	T	A	R
I	A	D	E	L
A	R	E	A	A
N	D	I	N	A

Tabla 3. Transposición con clave 5
Fuente: propia

Analicemos ¿Qué tienen de común el resultado y el texto plano o mensaje original?

Ahora bien, si se cambiamos la llave o clave, el resultado del criptograma cambia.

Texto plano	FUNDACION UNIVERSITARIA DEL AREA ANDINA
Algoritmo, clave o llave	7
Texto encriptado	FORAAUNSDANUIENDNTK-DAIAAICVRRNIEIEA

Al igual que en el caso anterior, construimos una matriz de 7 casillas en la cual escribimos el texto o mensaje en forma horizontal y obtenemos el mensaje encriptado al escribirlo por columnas.

F	U	N	D	A	C	I
O	N	U	N	I	V	E
R	S	I	T	A	R	I
A	D	E	L	A	R	E
A	A	N	D	I	N	A

Tabla 4. Transposición con clave 7
Fuente: propia

Criptografía moderna

Al hablar de criptografía moderna se debe hablar de criptografía simétrica, asimétrica e híbrida. En este eje, nombraremos las características básicas de cada una de ellas, en semestres posteriores se trabajará a profundidad este tema.

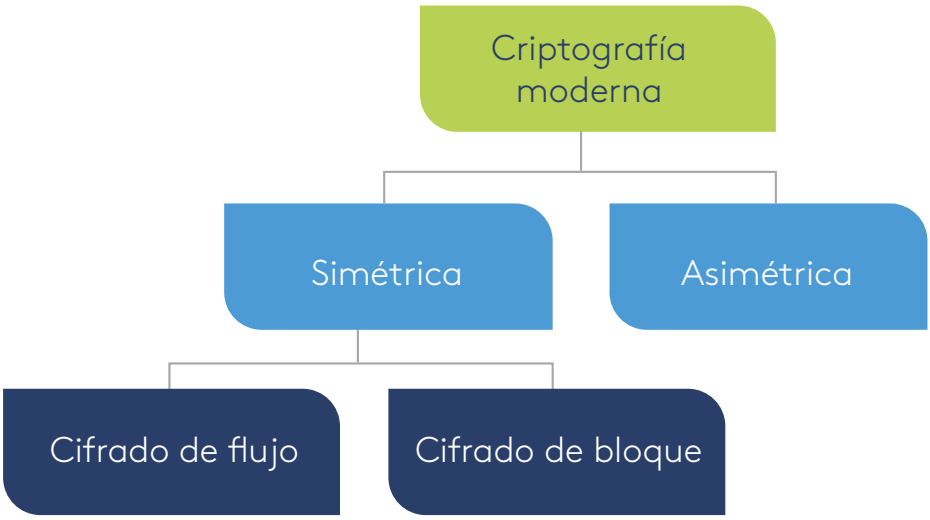


Figura 4. Criptografía moderna
Fuente: propia

La criptografía simétrica es aquella que utiliza una única clave para cifrar y descifrar el mensaje, dicha clave debe ser conocida tanto por el emisor como por el receptor, este intercambio de clave genera mayor debilidad, pues se hace propensa la interceptación de dicha clave.

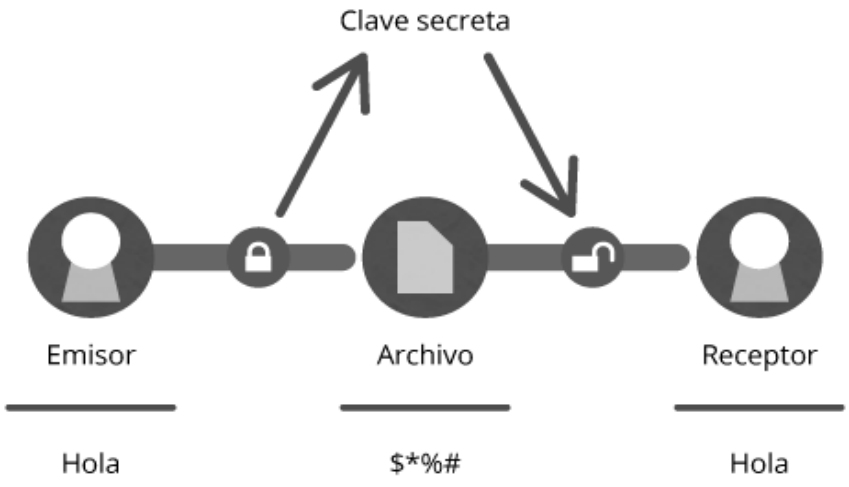


Figura 5. Criptografía simétrica
Fuente: https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

La criptografía asimétrica, se basa en el uso de dos claves o llaves, una llave privada que no se difunde, y una llave pública que se puede difundir sin ningún problema.

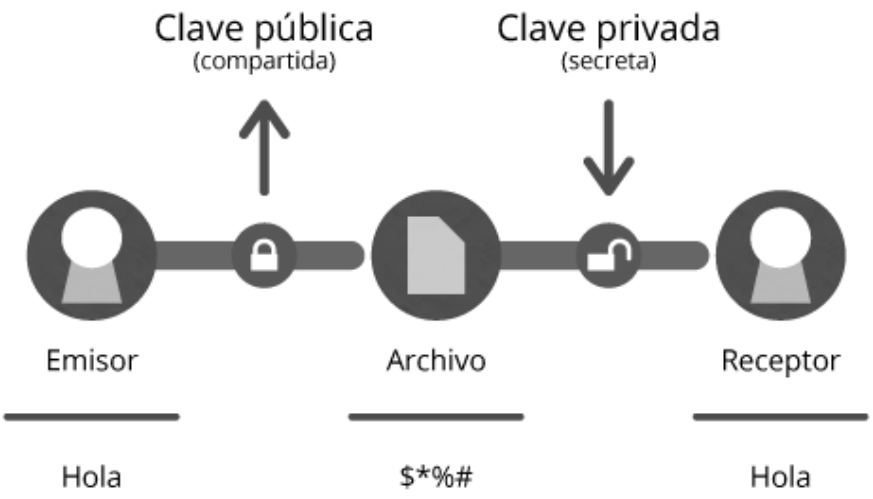


Figura 6. Criptografía asimétrica
Fuente: https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

Video

Los invito a ver el video Cápsula "Sistemas de cifras con clave pública" el cual explica el funcionamiento de la criptografía asimétrica.

Sistemas de cifras con clave pública

https://youtu.be/On1clzor4x4

Instrucción

Ahora realice la lectura del capítulo 4 del texto La seguridad de los datos de carácter personal.

La seguridad de los datos de carácter personal.

Emilio del Peso Navarro y Miguel Ramos González.

Ciclo de vida de la seguridad informática

Lectura recomendada

Para dar inicio a este tema los invito a leer los capítulos 5, 6, 7 y 8 de la norma ISO 27001, los cuales nos ayudaran a entender el ciclo de mejora continua PHVA y los procedimientos necesarios para generar un proceso adecuado de Gestión de la seguridad de la información.

Norma ISO 27001 SGSI - Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información (SGSI) – Requisitos.

Norma Técnica Colombiana

Como se mencionó en el primer eje del conocimiento, existen varios estándares, normas y leyes a nivel de seguridad informática, esta últimas se aplican de acuerdo al país y a su legislación, los mecanismos de derechos y protección a la información que son utilizadas con las TIC para su tratamiento, divulgación o manejo.

Las normas ISO juegan un papel importante, ya que estas se pueden adecuar a cualquier organización o entidad, no importa el país de procedencia, emplean mecanismos adecuados y estandarizados para brindar una eficiente seguridad informática, el sistema que existe bajo esta norma se denomina ISO 27001 – SGSI.

Esta norma ISO, se basa en el ciclo de vida o de mejora continua PHVA o PDCA (por sus siglas en inglés, Plan-Do-Check-Act), ya que esta se puede integrar fácilmente con otras normas, si ya están implementadas como: SGC (ISO 9001) y SGMA (14001).

TIC
Tecnologías de la información y la comunicación.

ISO
Organización internacional de estándares.

SGSI
Sistema de Gestión de la Seguridad de la Información

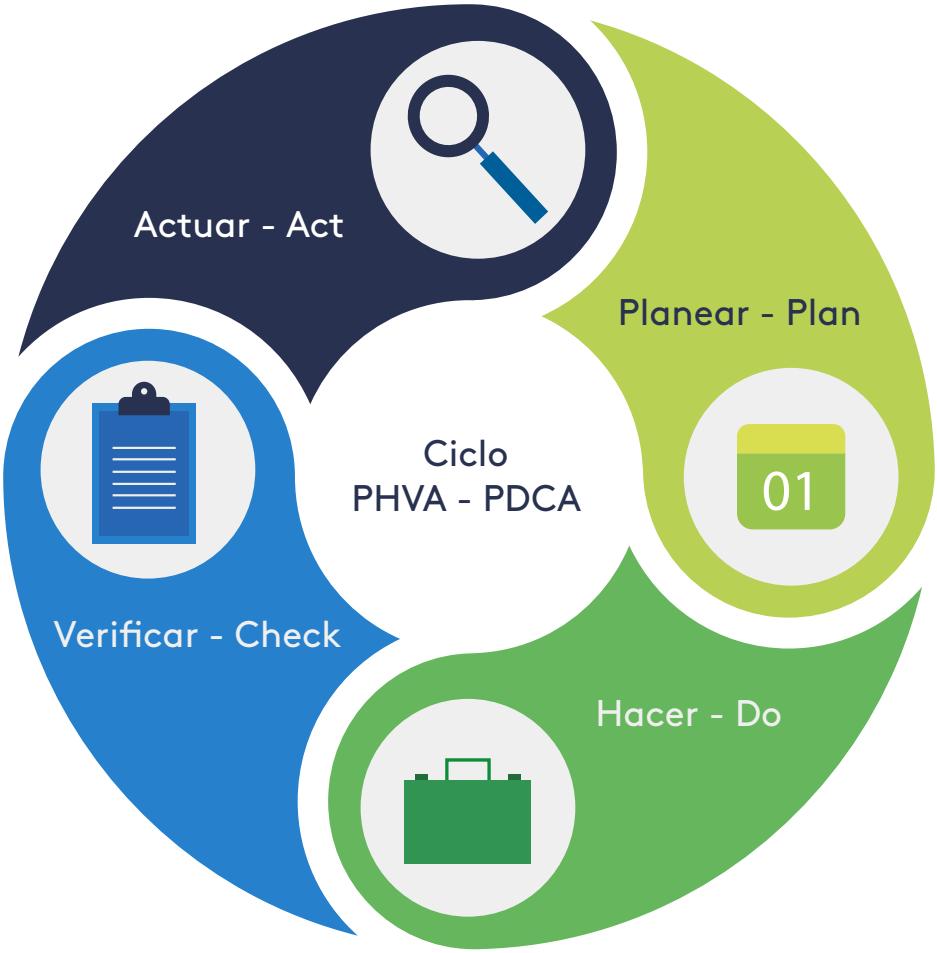


Figura 7. Ciclo de mejora continua PHVA- PDCA
Fuente: propia

Video

Para reafirmar los conceptos, los invito a ver la video cápsula "PHVA ciclo de mejora continua", la cual explica cada paso del proceso.

Video Capsula "PHVA ciclo de mejora continua"

https://youtu.be/qWz6pY7CYUE

Observe detalladamente el siguiente mapa conceptual

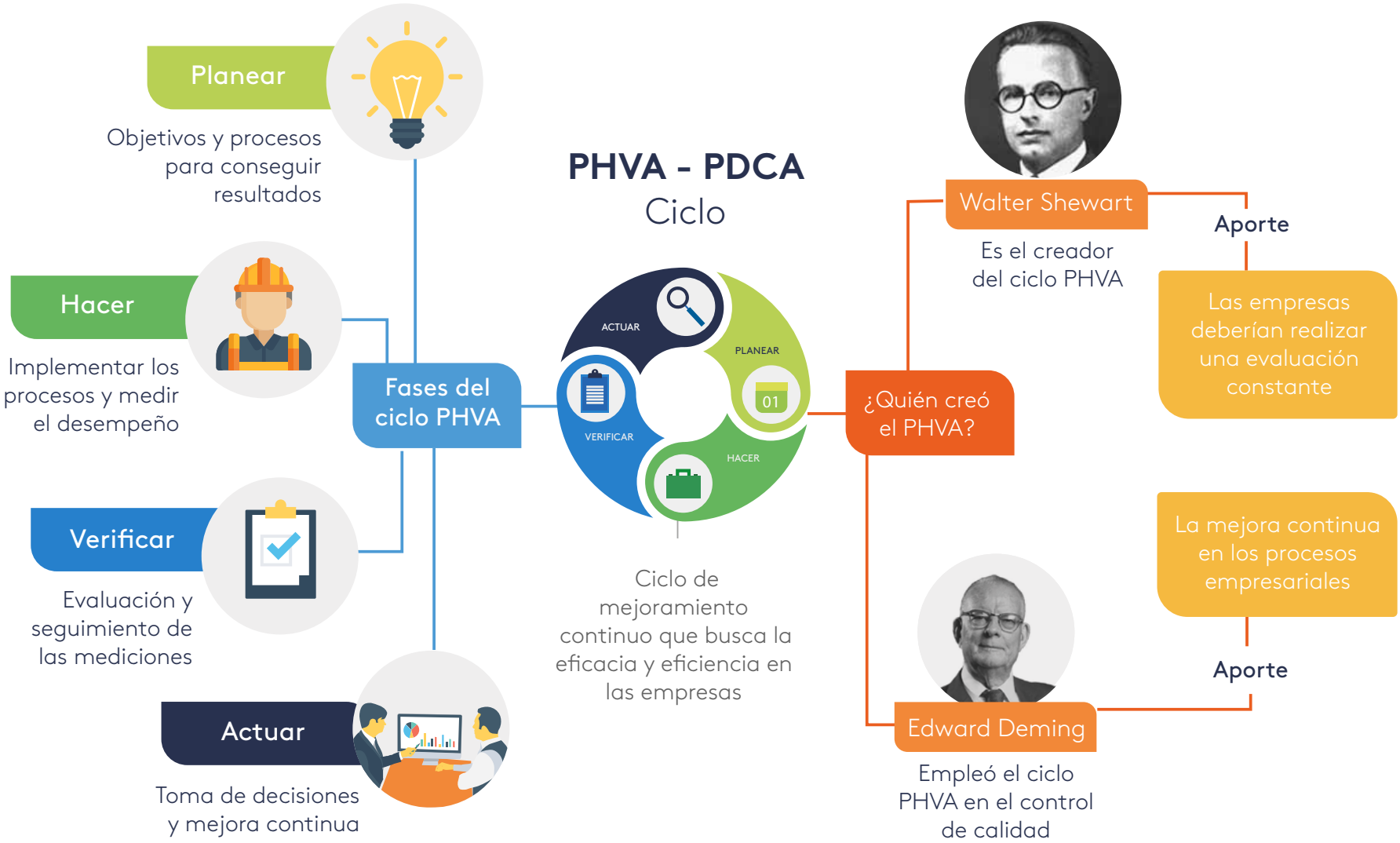


Figura 8. Ciclo PHVA
Fuente: propia

Un SGSI se implementa para gestionar riesgos de seguridad de la información, fundamentado en UNE-ISO/IEC 27001: 2013 (certificable para organizaciones), al igual se suma la serie de la ISO 27002 (no certificable), que son el conjunto de controles de la seguridad de la Información.

Figura 9. Sistema de Gestión de la Seguridad de la Información - SGSI
Fuente: propia

El ciclo de vida para un sistema de seguridad informática, es el proceso mediante el cual, se mantiene durante el tiempo la seguridad informática dentro de la organización, está conformado por un conjunto de fases similar al ciclo de mejora continua PHVA - PDCA de las normas ISO, y se toma de referencia para sostener el sistema que permite aplicar el método continuo para mitigar los riesgos.

Figura 10. Ciclo de vida de la seguridad informática
Fuente: propia

Fase de evaluación (ASSESS)

En esta fase, se debe realizar un análisis de riesgos, el cual permite emplear las metodologías *Magerit, Octave y Mehari* u otros métodos que permita su identificación, la principal importancia en esta fase es la de permitir detectar las debilidades y fortalezas en la seguridad informática, como, por ejemplo: revisión de aplicaciones, pentesting (pruebas de penetración a sistemas informáticos), análisis y evaluación de vulnerabilidades, auditorias, etc.

Para administrar los riesgos se debe tener en cuenta los procesos definidos por la AS/NZS 4360.

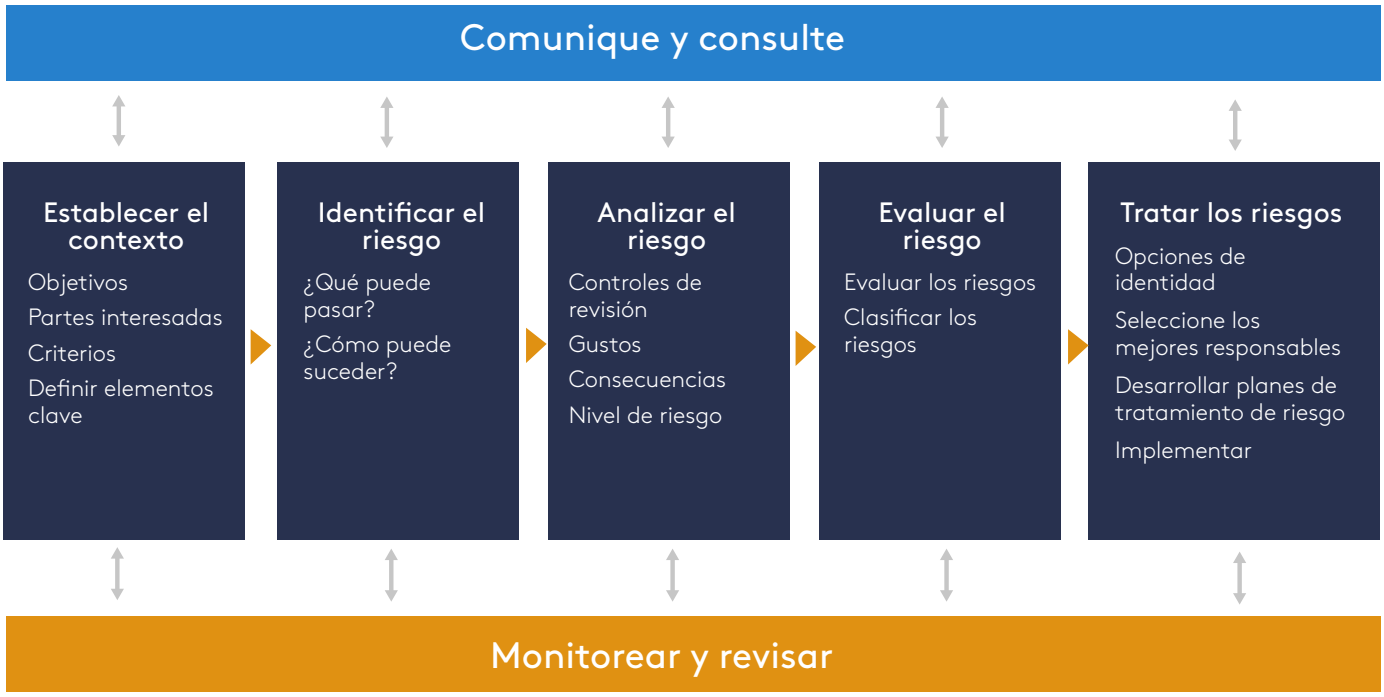


Figura 11. Procesos para la administración de riesgos (AS/NZS 4360)
Fuente: propia

Ventajas de realizar el análisis o identificación de riesgos:

- Realizar acciones (proactivas y reactivas).
- Administrar el riesgo permite establecer el método lógico y sistemático para establecer el contexto de identificar, analizar y evaluar el tratamiento a seguir, monitorear y comunicar los riesgos asociados con relación a los procesos o acción con una actividad para minimizar pérdidas e impactos dentro de la empresa.
- La detección de debilidades se puede determinar según el estado de la seguridad en dos áreas principales:
  - Técnica: consiste en aplicar la evaluación desde la seguridad física, el diseño de la seguridad en redes, hasta asociar una matriz de habilidades técnicas
  - No Técnica: aplica la evaluación de las políticas de la organización.

Acciones proactivas
Toma de iniciativas tendientes a mejorar y prevenir incidentes.

Acciones reactivas
Acciones tomadas ante un incidente.

- Permite realizar la revisión de otras áreas como: seguridad exterior, seguridad de la basura, seguridad en el edificio, revisión de passwords, ingeniería social, clasificación de los datos, entre otros.

Fase de diseño (DESIGN)

La fase de diseño, consiste en desarrollar actividades tales como la implementación de configuraciones de seguridad efectiva, basadas en los estándares de la industria, esto, con el fin de evitar que sucedan acciones indeseables o fallas en los sistemas informáticos, para ello se hace indispensable la aplicación de buenas prácticas.

Esta fase también permite la revisión de políticas que se necesitan implementar como:

- ¿Todos los empleados necesitan de internet?
- ¿Se presentan inconvenientes con el uso de la red o correos electrónicos?
- ¿Qué empleados están utilizando información confidencialidad o privada?
- ¿Cuáles empleados acceden de manera remota a la organización?
- ¿Qué empleados requieren dependencia de los recursos informáticos?

Las políticas definen cuáles o qué prácticas son aceptadas o no dentro de la organización. Dentro del diseño se debe considerar los Logs en los firewall, determinar si requiere la implementación de IDS o de IPS, al igual que el uso de firmas digitales para envió de documentos.

Finalmente, dentro de la fase de diseño se debe contemplar la formación a las personas dentro de la organización (planes de capacitación).

Logs
Hace referencia a los informes que se generan ante diversos eventos.

Firewall o corta fuego
Elemento de seguridad lógico y/o físico.

IDS
(Sistema de detección de intrusos) Programa que permite detectar accesos no autorizados.

IPS
(Sistema de prevención de intrusos) Es un software que ejerce el control de acceso a la red.

Ejemplo

Algunas actividades de esta fase de diseño son:

- Creación de eventos de seguridad, identificación y puestos de trabajo del personal.
- Publicación de noticias, boletines, artículos.
- Reuniones de socialización por departamentos o áreas.
- Envío de emails de concientización y colocar avisos en lugares estratégicos.
- Premiar a empleados por el buen uso de las políticas.
- Creación de un canal de sugerencias y comentarios, comunicados escritos, a través de internet, o intranet.

Fase de implementación (Deploy)

Esta fase permite al personal que se asigne poner en marcha los diferentes controles basados en la fase anterior sobre el diseño que se ha desarrollado. El cual permite adicionalmente inspeccionar, requerir o mejorar las tecnologías implementadas o planeadas.

Se debe elaborar un cronograma de las actividades planeadas, luego, hacer un seguimiento a estas para cuantificar porcentajes de avances o estados de lo que se lleva implementado con lo planeado.

Ejemplo de esto, antivirus, firewalls, proxys o filtrados de email, IDS, bloqueos de adjuntos, filtros para sitios webs no autorizados, análisis de vulnerabilidades, encriptación de email, VPN's, entre otros.

Fase de administración y soporte (manage & sopport)

Una vez que se haya evaluado, diseñado e implementando el sistema para la seguridad informática, se hace una administración y soporte al sistema para su mejoramiento continuo, en esta fase se debe observar las actividades normales y reaccionar ante incidentes o eventuales anomalías que impacten al sistema de seguridad. Se proporciona un monitoreo y alertas, así como las respuestas que se basan en el documento de políticas de seguridad definido.

Se debe tener un proceso claro respecto a cómo tratar un incidente cuando este ocurra o se esté presentando, encontrar el problema y aplicar acciones correctivas o

preventivas, realizar prácticas forenses, determinar la responsabilidad y la causa del problema.

Para el manejo de un incidente se deben considerar los siguientes factores: organización, identificación, encapsulamiento, erradicación y recuperación, además, se debe contar con documentos de lecciones aprendidas.

Incidente

Evento repentino no deseado, que causa mal funcionamiento del sistema o caída del mismo.

Capacitación continua

Finalmente, como todo sistema, debe estar dispuesto a tener capacitación continua de todos los actores que intervienen.

El ciclo de vida y ciclo de mejoramiento continuo, son procesos que deben ser constantes en todas sus fases a medida que se extiendan en toda la organización.

Antes de realizar la evaluación del segundo eje le invitamos a afianzar los conceptos aprendidos con algunas actividades interactivas propuestas en el portal Educaplay.

Visitar página

Crucigrama gestión de seguridad de la información https://www.educaplay.com/es/recursoseducativos/2119901/gestion_de_seguridad_enla_info.htm

Sopa de letras Pilares de la seguridad

https://www.educaplay.com/es/recursoseducativos/626734/pilares_seguridad_de_la_informacion.htm

Test Norma ISO 27001

https://www.educaplay.com/es/recursoseducativos/3767/norma_iso_27001.htm

Instrucción

Por último y para finalizar los invito a desarrollar de forma colaborativa la evaluación del segundo eje.

Figura 12. Seguridad informática
Fuente: www.shutterstock.com

BIBLIOGRAFÍA

Álvarez, M. y Pérez, G. (2004). *Seguridad informática para empresas y particulares*. Madrid: McGraw-Hill

Austin, R. y Darby, C. (2004). *El mito de la seguridad informática*. Madrid: Ediciones Deusto - Planeta de Agostini Profesional y Formación S.L.

Baca, U. G. (2016). Introducción a la seguridad informática. México: Grupo Editorial Patria.

Chicano, T. (2014). *Gestión de incidentes de seguridad informática (MF0488_3)*. Madrid: IC Editorial.

Chicano, T. (2014). *Auditoría de seguridad informática (MF0487_3)*. Madrid: IC Editorial.

Costas, S. J. (2014). *Seguridad informática*. Madrid: RA-MA Editorial.

Costas, S. (2014). Mantenimiento de la seguridad en sistemas informáticos. Madrid: RA-MA Editorial.

Escrivá, G., Romero, S. y Ramada, D. (2013). *Seguridad informática*. Madrid: Macmillan Iberia, S.A.

Ficarra, F. (2006). Antivirus y seguridad informática: el nuevo. *Revista Latinoamericana de Comunicación CHASQUI*.

Giménez, A. J. F. (2014). *Seguridad en equipos informáticos (MF0486_3)*. Madrid: IC Editorial.

Gómez, F. y Fernández, R. (2015). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad*. Madrid: AENOR - Asociación Española de Normalización y Certificación.

Gómez, V. (2014). *Auditoría de seguridad informática*. Madrid: RA-MA Editorial.

Gómez, V. (2014). *Gestión de incidentes de seguridad informática*. Madrid: RA-MA Editorial.

Hernández, E. (2016). *La criptografía*. Madrid: Editorial CSIC Consejo Superior de Investigaciones Científicas.

Lamadrid, V., Méndez, G. y Díaz, H. (2009). *CERT-MES: sitio Web de seguridad informática para REDUNIV*. La Habana: Editorial Universitaria.

BIBLIOGRAFÍA

McClure, S., Scambray, J. y Kurtz, G. (2010). *Hackers 6: secretos y soluciones de seguridad en redes*. México: McGraw-Hill Interamericana.

Molina, M. (2000). *Seguridad de la información*. *Criptología*. Córdoba: El Cid Editor.

Paredes, F. (2009). *Hacking*. Córdoba: El Cid Editor | apuntes.

UNED. (2014). *Procesos y herramientas para la seguridad de redes*. Madrid: Universidad Nacional de Educación a Distancia.

Roa, B. (2013). *Seguridad informática*. Madrid: McGraw-Hill

Sanz, M. (2008). *Seguridad en linux: guía práctica*. Madrid: Editorial Universidad Autónoma de Madrid.

Zayas, D. y Sánchez, R. (2010). Sistema de apoyo al entrenamiento en seguridad informática: SEGURIN. La Habana: Editorial Universitaria.