

“AÑO DE LA UNIVERSALIZACIÓN DE LA SALUD”.



**UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE
AREQUIPA**

**ESCUELA PROFESIONAL DE CIENCIA DE LA
COMPUTACIÓN
SEGURIDA EN COMPUTACIÓN**

Lab 1 - Criptografía

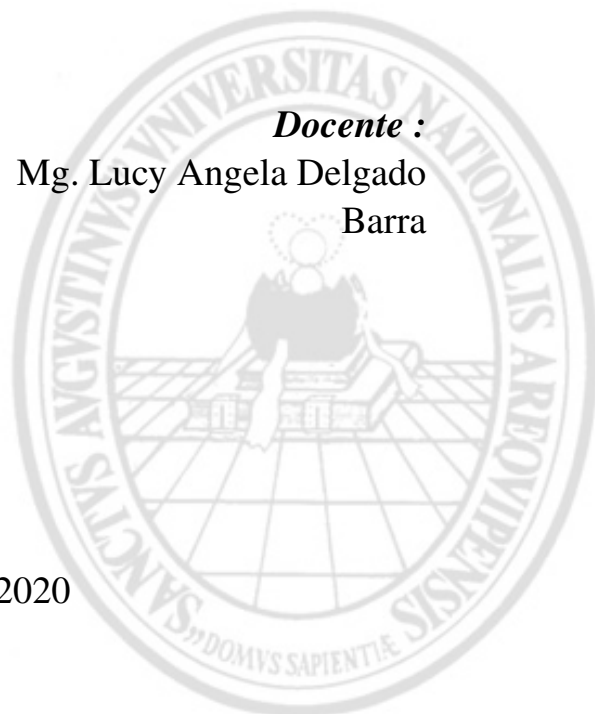
Alumnos:

Miguel Alexander, Herrera Cooper

Docente :

Mg. Lucy Angela Delgado
Barra

30 de septiembre de 2020



Índice

1. Actividades	2
1.1. Ejercicio 1	3
1.2. Ejercicio 2	4
1.3. Ejercicio 3	5
1.4. Ejercicio 4	6
1.5. Ejercicio 5	7
1.6. Ejercicio 6	8
1.7. Ejercicio 7	9
1.8. Ejercicio 8	10
1.9. Ejercicio 9	11
2. CONCLUSIONES	12
3. Cuestionario Final	13
3.1. Ejercicio 1	13
3.1.1. Protección y seguridad de los datos	13
3.1.2. Criptografía	13
3.1.3. Seguridad y fortificación de redes	13
3.1.4. Seguridad en aplicaciones informáticas, programas y bases de datos . .	13
3.1.5. Gestión de seguridad en equipos y sistemas informáticos	13
3.1.6. Informática forense	14
3.1.7. Ciberdelito	14
3.1.8. Ciberseguridad	14
3.2. Ejercicio 2	14
3.2.1. Gestión de la seguridad de la información	14
3.2.2. Asesoría y auditoría de la seguridad	14
3.2.3. Continuidad de negocio	14
3.2.4. Buen gobierno	15
3.2.5. Comercio electrónico	15
3.2.6. Legislación relacionada con seguridad	16
3.3. Ejercicio 3	16
3.4. Ejercicio 4	17
3.5. Ejercicio 5	17
4. Referencias	18

1. Actividades

Sobre el texto claro mostrado a continuación:

Hay golpes en la vida, tan fuertes. . . ¡Yo no sé!
Golpes como del odio de Dios; como si ante ellos,
la resaca de todo lo sufrido
se empozara en el alma. . . ¡Yo no sé!

Son pocos; pero son. . . Abren zanjas oscuras
en el rostro más fiero y en el lomo más fuerte.

Serán tal vez los potros de bárbaros Atilas;
o los heraldos negros que nos manda la Muerte.

Son las caídas hondas de los Cristos del alma
de alguna fe adorable que el Destino blasfema.
Esos golpes sangrientos son las crepitaciones
de algún pan que en la puerta del horno se nos quema.

Y el hombre. . . Pobre. . . ¡pobre! Vuelve los ojos, como
cuando por sobre el hombro nos llama una palmada;
vuelve los ojos locos, y todo lo vivido
se empoza, como charco de culpa, en la mirada.

Hay golpes en la vida, tan fuertes. . . ¡Yo no sé!

Implementar las siguientes operaciones de preprocesamiento, en cada caso debe mostrar el código de la solución y la salida parcial resultante en cada caso.

1.1. Ejercicio 1

Realizar las siguientes sustituciones: j x i, h x i, ñ,x n, k x l, u x v, w x,v, y x z

Resolución

```

1 def func1():
2     f = open("HERALDOSNEGROS_pre2.txt", encoding="utf8")
3     g = open("HERALDOSNEGROS_pre1.txt", "w")
4
5     for linea in f:
6         for x in linea:
7             if(x=="j"):
8                 x="i"
9             if(x=="h"):
10                x="i"
11            if(x==" "):
12                x="n"
13            if(x=="k"):
14                x="l"
15            if(x=="u"):
16                x="v"
17            if(x=="w"):
18                x="v"
19            if(x=="y"):
20                x="z"
21            g.write(x)
22
23     g.close()
24     f.close()

```

```

1 Haz golpes en la vida, tan fvertes... Yo no se!
2 Golpes como del odio de Dios; como si ante ellos,
3 la resaca de todo lo svfrido
4 se empozara en el alma... Yo no se!
5
6 Son pocos; pero son... Abren zancias oscvras
7 en el rostro mas fiero z en el lomo mas fverte.
8
9 Seran tal vez los potros de barbaros Atilas;
10 o los ieraldos negros qve nos manda la Mverte.
11
12 Son las caidas iondas de los Cristos del alma
13 de algvna fe adorable qve el Destino blasfema.
14 Esos golpes sangrientos son las crepitaciones
15 de algvn pan qve en la pverta del iorno se nos qvema.
16
17 Y el iombre... Pobre... pobre ! Vvelve los oios, como
18 cvando por sobre el iombro nos llama vna palmada;
19 vvelve los oios locos, z todo lo vivido
20 se empoza, como ciarco de cvlpa, en la mirada.
21
22 Haz golpes en la vida, tan fvertes... Yo no se!

```

1.2. Ejercicio 2

Elimine las tildes

Resolución

```
1 def func2():
2     f = open("init.txt", encoding="utf8")
3     g = open("HERALDOSNEGROS_pre.txt", "w")
4
5     for linea in f:
6         for x in linea:
7             if(x==" "):
8                 x="a"
9             if(x==" "):
10                x="e"
11            if(x==" "):
12                x="i"
13            if(x==" "):
14                x="o"
15            if(x==" "):
16                x="u"
17            g.write(x)
18
19     g.close()
20     f.close()
```

```
1 Hay golpes en la vida, tan fuertes... Yo no se!
2 Golpes como del odio de Dios; como si ante ellos,
3 la resaca de todo lo sufrido
4 se empozara en el alma... Yo no se!
5
6 Son pocos; pero son... Abren zanjas oscuras
7 en el rostro mas fiero y en el lomo mas fuerte.
8
9 Seran tal vez los potros de barbaros Atilas;
10 o los heraldos negros que nos manda la Muerte.
11
12 Son las caidas hondas de los Cristos del alma
13 de alguna fe adorable que el Destino blasfema.
14 Esos golpes sangrientos son las crepitaciones
15 de algun pan que en la puerta del horno se nos quema.
16
17 Y el hombre... Pobre... pobre ! Vuelve los ojos, como
18 cuando por sobre el hombro nos llama una palmada;
19 vuelve los ojos locos, y todo lo vivido
20 se empoza, como charco de culpa, en la mirada.
21
22 Hay golpes en la vida, tan fuertes... Yo no se!
```

1.3. Ejercicio 3

Convierta todas las letras a mayúsculas

Resolución

```

1 def func3():
2     f = open("HERALDOSNEGROS_pre1.txt", encoding="utf8")
3     g = open("HERALDOSNEGROS_pre3.txt", "w")
4     for linea in f:
5         for x in linea:
6             z = ord(x)
7             if(z>=97 and z<=122):
8                 z-=32
9             x = str(chr(z))
10            g.write(x)
11
12
13    g.close()
14    f.close()

```

```

1 HAZ GOLPES EN LA VIDA, TAN FVERTES YO NO SE!
2 GOLPES COMO DEL ODIO DE DIOS; COMO SI ANTE ELLOS,
3 LA RESACA DE TODO LO SVFRIDO
4 SE EMPOZARA EN EL ALMA YO NO SE!
5
6 SON POCOS; PERO SON ABREN ZANIAS OSCVRAS
7 EN EL ROSTRO MAS FIERO Z EN EL LOMO MAS FVERTE.
8
9 SERAN TAL VEZ LOS POTROS DE BARBAROS ATILAS;
10 O LOS IERALDOS NEGROS QVE NOS MANDA LA MVERTE.
11
12 SON LAS CAIDAS IONDAS DE LOS CRISTOS DEL ALMA
13 DE ALGVNA FE ADORABLE QVE EL DESTINO BLASFEMA.
14 ESOS GOLPES SANGRIENTOS SON LAS CREPITACIONES
15 DE ALGVN PAN QVE EN LA PVERTA DEL IORNO SE NOS QVEMA.
16
17 Y EL IOMBRE POBRE POBRE ! VVELVE LOS OIOS, COMO
18 CVANDO POR SOBRE EL IOMBRO NOS LLAMA VNA PALMADA;
19 VVELVE LOS OIOS LOCOS, Z TODO LO VIVIDO
20 SE EMPOZA, COMO CIARCO DE CVLPA, EN LA MIRADA.
21
22 HAZ GOLPES EN LA VIDA, TAN FVERTES YO NO SE!

```

1.4. Ejercicio 4

4. Elimine los espacios en blanco y los signos de puntuación

Resolución

```

1 def func4():
2     f = open("HERALDOSNEGROS_pre3.txt", encoding="utf8")
3     g = open("HERALDOSNEGROS_preFINAL.txt", "w")
4     for linea in f:
5         for x in linea:
6             if (x==" " or x==chr(46) or x=="," or x==" " or x==":" or x==";" or
7                 x==" " or x=="!"):
8                 x=""
9             g.write(x)
10    g.close()
11    f.close()

```

```

1 HAZGOLPESENLAVIDATANFVERTESYONOSE
2 GOLPESCOMODELODIEDIOSCOMOSIANTEELLOS
3 LARESACADETODOLOSVFRIDO
4 SEEMPOZARAENELALMAYONOSE
5
6 SONPOCOSPERSOSONABRENZANIASOSCVRAS
7 ENELROSTROMASFIEROZENELLOMOMASFVERTE
8
9 SERANTALVEZLOSPOTROSDEBARBAROSATILAS
10 OLOSIERALDOSNEGROSQVENOSMANDALAMVERTE
11
12 SONLASCAIDASIONDASDELOSCRISTOSDELALMA
13 DEALGVNAFEADORABLEQVEELDESTINOBLASFEMA
14 ESOGOLPESSANGRIENTOSONLASCREPITACIONES
15 DEALGVNPANQVEENLAPVERTADELIORNOSENOSQVEMA
16
17 YELIOMBREPOBREPOBREVVELVELOSOIOSCOMO
18 CVANDOPORSOBREELIOMBRONOSLLAMAVNAPALMADA
19 VVELVELOSOIOSLOCOSZTODOLOVIVIDO
20 SEEMPOZACOMOCIARCODECVLPAENLAMIRADA
21
22 HAZGOLPESENLAVIDATANFVERTESYONOSE

```

Guarde el resultado en el archivo “HERALDOSNEGROS_pre.txt”

1.5. Ejercicio 5

Abra el archivo generado e implementar una función que calcule una tabla de frecuencias para cada letra de la 'A' a 'Z'. La función deberá definirse como *frecuencias(archivo)* deberá devolver un diccionario cuyos índices son las letras analizadas y cuyos valores son las frecuencias de las mismas en el texto (número de veces que aparecen). Reconozca en el resultado obtenido los cinco caracteres de mayor frecuencia

Resolución

```
1 def frecuencias(archivo):
2     f = open(archivo+".txt",encoding="utf8")
3     c=[]
4     for i in range(26):
5         c.append([])
6         for j in range(2):
7             c[i].append(None)
8     for i in range(26):
9         c[i][0]=str(chr(i+65))
10        c[i][1]=0
11    for linea in f:
12        for x in linea:
13            z=ord(x)
14            if(z!=10):
15                z=z-65
16                c[z][1]=c[z][1]+1
17    c.sort(key=lambda frecuencia: frecuencia[1],reverse=True)
18    for i in range(26):
19        print(c[i])
20    print("Las letras mas frecuentes son: ")
21    for i in range(5):
22        print(c[i])
23    f.close()
```

```
1 ['O', 83]
2 ['E', 74]
3 ['A', 65]
4 ['S', 59]
5 ['L', 47]
6 ['N', 36]
7 ['R', 33]
8 ['D', 27]
9 ['V', 27]
10 ['I', 26]
11 ['M', 20]
12 ['T', 18]
13 ['P', 17]
14 ['C', 16]
15 ['B', 10]
16 ['G', 8]
17 ['Z', 8]
18 ['F', 7]
19 ['Q', 4]
20 ['Y', 4]
21 ['H', 2]
22 ['J', 0]
23 ['K', 0]
```



```

24 ['U', 0]
25 ['W', 0]
26 ['X', 0]
27 Las letras mas frecuentes son:
28 ['O', 83]
29 ['E', 74]
30 ['A', 65]
31 ['S', 59]
32 ['L', 47]

```

1.6. Ejercicio 6

Aplicar el método Kasiski, que recorre el texto preprocesado y halla los trigramas en el mismo (sucesión de tres letras seguidas que se repiten) y las distancias (número de caracteres entre ellos) entre los trigramas

Resolución

```

1 def Kasiski(archivo):
2     f = open(archivo+".txt",encoding="utf8")
3     c=[]
4     cont=0
5     ini=0
6     fin=0
7     dist=0
8     for linea in f:
9         for i in range(0,len(linea)):
10            tri=linea[i:3+i]
11            ini=i+3
12            for j in range(i,len(linea),3):
13                auxtri=linea[j:3+j]
14                if(tri==auxtri):
15                    dist=(j-ini)
16                    if(dist!=-3):
17                        dist=0
18                    c.append([])
19                    for k in range(2):
20                        c[cont].append(None)
21                    c[cont][0]=tri
22                    c[cont][1]=dist
23                    ini=j+3
24                    cont=cont+1
25                    dist=0
26     f.close()
27     for i in range(len(c)):
28         if(c[i][1]!=0):
29             print(c[i])

```

```

cooper@cooper-legion-y545:
['SON', 9]
['DAS', 3]
['SDE', 9]
['DEL', 9]

```

1.7. Ejercicio 7

Volver a preprocesar el archivo cambiando cada carácter según UNICODE-8

Resolución

```
1 def unicode(archivo):
2     f = open(archivo+".txt", encoding = "utf8")
3     g = open("HERALDOSNEGROS_pre8.txt", "w")
4     for linea in f:
5         for j in linea:
6             g.write(str(ord(j)))
7     g.close()
8     f.close()
```

```
726590717976806983697876658673686584657870866982846983897978798369107179768
069836779777968697679687379686968737983677977798373657884696976767983107665
826983656765686984796879767983867082736879108369697780799065826569786976657
677658979787983691010837978807967798380698279837978656682697890657873658379
836786826583106978697682798384827977658370736982799069786976767977797765837
086698284691010836982657884657686699076798380798482798368696665826665827983
658473766583107976798373698265766879837869718279838186697879837765786865766
577866982846910108379787665836765736865837379786865836869767983678273838479
836869766576776510686965767186786570696568798265667669818669697668698384737
879667665837069776510698379837179768069838365787182736978847983837978766583
678269807384656773797869831068696576718678806578818669697876658086698284656
869767379827879836978798381866977651010896976737977668269807966826980796682
698686697686697679837973798367797779106786657868798079828379668269697673797
766827978798376766577658678658065767765686510868669768669767983797379837679
677983908479687976798673867368791083696977807990656779777967736582677968696
786768065697876657773826568651010726590717976806983697876658673686584657870
8669828469838979787983691010
```

1.8. Ejercicio 8

Volver a preprocesar el archivo cambiando cada carácter según UNICODE-8230

Resolución

1.9. Ejercicio 9

Volver a preprocesar el archivo insertando la cadena AQUÍ cada 20 caracteres, el texto resultante deberá contener un número de caracteres que sea múltiplo de 4, si es necesario rellenar al final con caracteres X según se necesite

Resolución

```

1 def aqui(archivo):
2     f = open(archivo+".txt",encoding="utf8")
3     g = open("HERALDOSNEGROS_pre9.txt","w")
4     cont=0
5     conttotal=0
6     for linea in f:
7         for j in linea:
8             cont=cont+1
9             conttotal=conttotal+1
10            if(cont==21):
11                cont=1
12                conttotal=conttotal+4
13                g.write("AQUI")
14                g.write(j)
15            else:
16                g.write(j)
17        conttotal=conttotal%4
18        if(conttotal!=0):
19            g.write("X"*conttotal)
20        g.close()
21        f.close()
22
23 aqui("HERALDOSNEGROS_pre")

```

```

1 HAZGOLPESENLAVIDATANAQUIIFVERTESYONOSE
2 GOLPESAQUICOMODELODIODEDIOSCOMAQUIIOSIANTEELLOS
3 LARESACAQUIADETODOLOSVFRIDO
4 SEEAQUIMPOZARAENELALMAYONOSAQUIE
5
6 SONPOCOSPERSONABAQUIIRENZANIASOSCVRAS
7 ENEAQUILROSTROMASFIEROZENELAQUILOMOMASFVERTE
8
9 SERANAQUITALVEZLOSPOTROSDEBARAQUIIBAROSATILAS
10 OLOSIERAAQUILDOSNEGROSQVENOSMANDAQUIALAMVERTE
11
12 SONLASCAIAQUIDASIONDASDELOSCRISTOAQUISDELALMA
13 DEALGVNAFEAAQUIDORABLEQVEELDESTINOBAQUILASFEMA
14 ESOGOLPESSAAQUINGRIENTOSONLASCREPIAQUITACIONES
15 DEALGVNPANQAQUIVEENLAPVERTADELIORNOAQUISENOSQVEMA
16
17 YELIOMBRAQUIIEPOBREPOBREVVELVELOSAQUIOIOSCOMO
18 CVANDOPORSOAQUIIBREELIOMBRONOSLLAMAVAQUINAPALMADA
19 VVELVELOSAQUIIOSLOCOSZTODOLOVIVIDAQUIO
20 SEEMPOZACOMOCIARCOAQUIDECVLPAENLAMIRADA
21
22 HAQUIAZGOLPESENLAVIDATANFAQUIIVERTESYONOSE
23
24 XX

```

2. CONCLUSIONES

1. Debido a las cambiantes condiciones y nuevas plataformas de computación disponibles, es vital el desarrollo de documentos y directrices que orienten a los usuarios en el uso adecuado de las tecnologías para aprovechar mejor sus ventajas.
2. El auge de la interconexión entre redes abre nuevos horizontes para la navegación por Internet y con ello, surgen nuevas amenazas para los sistemas computarizados, como son la pérdida de confidencialidad y autenticidad de los documentos electrónicos.
3. La Criptografía es una disciplina/tecnología orientada a la solución de los problemas relacionados con la autenticidad y la confidencialidad, y provee las herramientas idóneas para ello.
4. Amenazas más sutiles provienen de los controles inadecuados de la programación, como es el problema de los residuos, es decir, de la permanencia de información en memoria principal cuando un usuario la libera o, en el caso de dispositivos externos, cuando se borra incorrectamente.
5. Los usuarios son quienes deben elegir la conveniencia de una u otra herramienta para la protección de sus documentos electrónicos.
6. Los algoritmos criptográficos tienden a degradarse con el tiempo. A medida que transcurre el tiempo, los algoritmos de encriptación se hacen más fáciles de quebrar debido al avance de la velocidad y potencia de los equipos de computación.
7. Una técnica fraudulenta muy utilizada consiste en transferir información de un programa a otro mediante canales ilícitos, no convencionales (canales ocultos). El análisis del comportamiento de las amenazas a la seguridad de la información revela que la mayoría de los hechos se cometen por intrusos individuales. Un por ciento menor corresponde a incidentes protagonizados por grupos organizados, y en la punta de la pirámide, se ubican los casos de espionaje (industrial, económico, militar...).
8. Todos los algoritmos criptográficos son vulnerables a los ataques de fuerza bruta -tratar sistemáticamente con cada posible clave de encriptación, buscando colisiones para funciones hash, factorizando grandes números, etc.- la fuerza bruta es más fácil de aplicar en la medida que pasa el tiempo.

3. Cuestionario Final

3.1. Ejercicio 1

Describe los siguientes términos (áreas de la seguridad informática)

3.1.1. Protección y seguridad de los datos

Es la protección de datos contra accesos no autorizados y para protegerlos de una posible corrupción durante todo su ciclo de vida.

Seguridad de datos incluye conceptos como encriptación de datos, tokenización y prácticas de gestión de claves que ayudan a proteger los datos en todas las aplicaciones y plataformas de una organización.

3.1.2. Criptografía

Criptografía es la ciencia y arte de escribir mensajes en forma cifrada o en código. Es parte de un campo de estudios que trata las comunicaciones secretas, usadas, entre otras finalidades, para:

1. Autenticar la identidad de usuarios.
2. Autenticar y proteger el sigilo de comunicaciones personales y de transacciones comerciales y bancarias.
3. Proteger la integridad de transferencias electrónicas de fondos.

3.1.3. Seguridad y fortificación de redes

Tiene como objetivo fortalecer la red para poder tener un acceso seguro, ya que por la red pueden surgir ataques, entonces es necesario estudiar el estado y las características de la red de control, y a partir de ello saber como fortificarla para evitar los ataques valga la redundancia.

3.1.4. Seguridad en aplicaciones informáticas, programas y bases de datos

Se refiere a medidas de protección de la privacidad digital que se aplican para evitar el acceso no autorizado a los datos, los cuales pueden encontrarse en ordenadores, bases de datos, sitios web, etc.

3.1.5. Gestión de seguridad en equipos y sistemas informáticos

Los equipos informáticos ejecutan aplicaciones que manejan información importante, como datos financieros, o datos de carácter estratégico, suelen también controlar máquinas, tomar decisiones, entre otras actividades, entonces por ello es muy importante protegerlo, para prevenir ataques, lo mismo con los sistemas informáticos, todo aquellos que manejan información o realizan actividades.

3.1.6. Informática forense

Se encarga de analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial.

3.1.7. Ciberdelito

Es una infracción llevada a cabo a través de medios digitales. Esto quiere decir que, cualquier persona que utilice Internet, está expuesto a este tipo de delitos.

3.1.8. Ciberseguridad

Se trata de mitigar los riesgos que todo negocio en la red pueda tener. No es otra cosa que proteger toda la información de los equipos y almacenada en cualquier dispositivo y en la nube.

No solo sirve para prevenir sino también para dar confianza a los clientes. Además, ayuda al mercado a reducir el riesgo de exposición del usuario y los sistemas.

3.2. Ejercicio 2

Describe los siguientes términos (áreas de la seguridad de la información)

3.2.1. Gestión de la seguridad de la información

La seguridad de la información, según ISO 27001, consiste en la preservación de confidencialidad, integridad y disponibilidad, así como los sistemas implicados en su tratamiento, dentro de una organización. Entonces una gestión de la seguridad de la información implicaría:

- Compromiso de la dirección general de la organización.
- Elaboración de un plan de Gestión de Seguridad.
- Asignación de recursos, funciones y responsabilidades.
- Formación y concienciación del personal
- Establecer controles periódicos y mejoras.

3.2.2. Asesoría y auditoría de la seguridad

La auditoría continua garantiza que todo el software se actualiza a la última versión, se identifican y resuelven todas las anomalías en el rendimiento del sistema y se cumplen todos los requisitos de cumplimiento de seguridad. La monitorización constante asegura que cualquier comportamiento irregular sea inmediatamente identificado e investigado.

3.2.3. Continuidad de negocio

En temas de Continuidad de Negocio, la gestión y análisis de los riesgos es total. Es por ello que primeramente debemos conocer los Activos críticos de la organización, es decir, aquellos que son vitales para el funcionamiento de la empresa, sin los cuales no podría seguir operando y donde el Riesgo es Crítico.

Por ejemplo, los bancos no pueden darse el lujo de interrumpir su sistema informático, pues básicamente todas sus transacciones bancarias se registran y procesan a través de dicho sistema. Ante una amenaza de interrupción del sistema por un ataque informático, éste debe tener los cortafuegos, antivirus, antimalware, sistemas de seguridad, entre otros, adecuados y actualizados

En este contexto, surge la puesta en marcha del estándar propio de los Sistemas de Seguridad de la Información, que es la ISO 27001. El sitio web advisera.com la define como “una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. (...) Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001”

Por ello, la ISO 27001, junto a la norma ISO 22301, son básicas para la Gestión de Riesgos y la Continuidad de Negocio. La primera evalúa los problemas o incidentes potenciales que podrían afectar los sistemas de seguridad de la información dentro de la empresa, y la segunda garantiza que la empresa, a pesar del incidente, pueda seguir funcionando. Es por ello que en organizaciones como los bancos, empresas financieras, empresas del sector salud, entre otros, los planes de Continuidad de Negocio y de Sistemas de Seguridad de la Información, son fundamentales.

3.2.4. Buen gobierno

Es aquel que se ejerce de una manera objetivamente correcta, persiguiendo el cumplimiento de los intereses generales, y consiguiendo en un alto grado una buena gestión, alcanzando cotas muy aceptables de transparencia, eficacia, eficiencia, cumplimiento de la legalidad y un alto grado de satisfacción en el ciudadano.

3.2.5. Comercio electrónico

Es la compraventa y distribución de bienes y servicios a través de internet u otras redes informáticas.

Constituye un nuevo soporte para la actividad comercial porque carece de materialidad y de pautas físicas (espacio y tiempo) pero le da accesibilidad y rapidez. De tal modo que se pueden realizar transacciones todos los días del año a cualquier hora y en cualquier lugar del mundo.

3.2.6. Legislación relacionada con seguridad

Existe normativa legal que regula el diseño, operación, uso y administración de los sistemas de información.

Los requisitos normativos y contractuales de cada sistema de información deben estar debidamente definidos y documentados.

10 leyes de la Ciberseguridad:

1. Si alguien puede convencerle de que ejecute su programa en su equipo, dejará de ser su equipo.
2. Si alguien puede modificar el sistema operativo, dejará de ser su equipo.
3. Si alguien tiene acceso físico sin restricciones a su equipo, dejará de ser su equipo.
4. Si permite que alguien cargue programas en su sitio Web, dejará de ser su sitio Web.
5. Las contraseñas débiles anulan una seguridad fuerte.
6. Una máquina es tan segura como digno de confianza sea el administrador.
7. Los datos de cifrado son tan seguros como las claves de descifrado.
8. Un programa antivirus no actualizado es poco más seguro que no disponer del mismo.
9. El anonimato absoluto no es práctico en la vida real ni en la Web.
10. La tecnología no es una panacea.

3.3. Ejercicio 3

Describa alguna otra operación o función de preprocesamiento que se implemente sobre el texto claro en los criptosistemas, en que afecta la complejidad de estas funciones al desempeño del mismo

La manera más sencilla de cifrar un texto y crear por tanto un criptograma, consiste en cambiar de lugar las letras de ese texto en claro, es decir desordenándolas de forma que su lectura nos lleve a algo sin sentido. Con ello se logra el efecto de difusión pero, en cambio, su talón de Aquiles es que el criptograma contiene exactamente las mismas letras que el texto en claro y, por lo tanto, se manifiesta de forma patente en dicho criptograma la redundancia característica del lenguaje que aparece en el texto en claro.

En la criptografía clásica este método de cifra por permutación muestra un corto recorrido y, por lo tanto, conocemos muy pocos algoritmos. Los sistemas clásicos se centrarán preferentemente en el método de cifrado por sustitución.

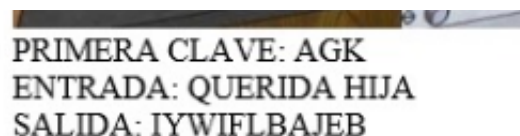
No sucederá lo mismo en la cifra moderna, orientada como es obvio a bits y a bytes, en donde la técnica de permutación se usa frecuentemente. Como ejemplo, baste nombrar al algoritmo DES, que presenta varias operaciones de permutación de bits, tanto en el texto en claro como en las claves de cada vuelta, e incluso en el algoritmo AES -actual estándar mundial de cifra simétrica-, dentro de la operación denominada ShiftRows, aunque en este caso la permutación se haga sobre bytes

3.4. Ejercicio 4

Describa la máquina enigma, luego muestre usando un simulador en internet la encriptación de la frase QUERIDA HIJA, para tres posiciones distintas de los rotores

Su fama se debe a haber sido adoptada por las fuerzas militares de Alemania desde 1930. Su facilidad de manejo y supuesta inviolabilidad fueron las principales razones para su amplio uso. Su sistema de cifrado fue finalmente descubierto y la lectura de la información que contenían los mensajes supuestamente protegidos es considerado, a veces, como la causa de haber podido concluir la Segunda Guerra Mundial al menos dos años antes de lo que hubiera acaecido sin su descifrado.

Para la encriptación de la frase QUERIDA HIJA, se usó un simulador web de la máquina enigma y se obtuvo el siguiente resultado:



PRIMERA CLAVE: AGK
ENTRADA: QUERIDA HIJA
SALIDA: IYWIFLBAJEB

3.5. Ejercicio 5

Describa la aplicación de Unicode-8

El estándar Unicode asigna un punto de código (un número) a cada carácter en todos los idiomas admitidos. UTF-8 permite codificar utilizando tamaños de datos de 8 bits y funciona bien con muchos de los sistemas operativos existentes.

Las referencias numéricas de caracteres especifican la posición del código de un carácter en el conjunto de caracteres del documento. Las referencias numéricas de caracteres pueden tener dos formas:

- La sintaxis "&#D;", donde D es un número decimal
- La sintaxis "&#xH;" o "&#XH;", donde H es un número hexadecimal (Para los números hexadecimales de referencias de caracteres numéricas no se distingue entre mayúsculas y minúsculas.)

Para el intervalo ASCII de caracteres, UTF-8 es idéntico a la codificación ASCII y permite un conjunto mayor de caracteres. Para scripts español y griego, sin embargo, UTF-8 puede necesitar dos bytes para cada carácter.

4. Referencias

1. <http://www.amenigma.com/> - Simulador Enigma
2. <https://www.tecnologia-informatica.com/que-es-la-criptografia/>
3. <https://www.powerdata.es/seguridad-de-datos>
4. <https://www.eadic.com/ciberseguridad-gestion-de-riesgos-y-la-continuidad-de-negocio/>
5. <https://ciberseguridad.com/normativa/espana/medidas/continuidad-negocio/>
6. <https://ecommerce-platforms.com/es/glossary/ecommerce>
7. http://www.adminso.es/index.php/1._Las_diez_leyes_inmutables_de_la_seguridad
8. <http://www.criptored.upm.es/crypt4you/temas/criptografiaclassica/leccion7.html>
9. https://www.periodni.com/es/codificacion_utf-8_unicode.html