VULNERACIÓN A LA PRIVACIDAD DE DOCUMENTOS ELECTRÓNICOS

Luisa Velásquez López [1]

[1] Instituto de Investigaciones en Informática
Universidad Mayor de "San Andrés" La paz – Bolivia

Correo electrónico: luisavlopez@gmail.com, luisavl@yahoo.es

RESUMEN

En la actualidad el tipo de tecnología que constituye la infraestructura de la información y comunicación, está cambiando significativamente, el número y tipo de dispositivos, servicios y variedades que integran la infraestructura de acceso, se ha multiplicado. Como consecuencia de estos cambios el volumen de información que se intercambia ha aumentado significativamente.

La información hoy en día es un activo muy valioso para casi todas las organizaciones y como tal debe estar contemplada por la seguridad informática. Por otro lado, la creciente interconexión masiva y global, de los sistemas y las redes de información ha vuelto vulnerable y expone a una cantidad creciente y variedad de amenazas de la información. Esto conlleva a que deben abordarse nuevos retos en materia de seguridad. En ese sentido la seguridad informática pretende eliminar parcial o total las pérdidas que pudieran surgir.

El intercambio de documento mediante correo electrónico, simplifica y acelera el intercambio de información. Sin embargo, cuando la información es importante o confidencial, se debe garantizar la seguridad de la misma, mantener un control de los documentos dentro y fuera de la red, protegiendo eficazmente dicha información asignando contraseñas y/o claves.

Si bien la información almacenada en una computadora personal es responsabilidad del encargado del manejo de los mismos, garantizando la seguridad, evitando alteraciones, perdidas, tratamiento o acceso no autorizado, no se tiene la plena seguridad de que ello sea así, de ahí la necesidad de tener modelos criptográficos adecuados.

PALABRAS CLAVE

Privacidad, vulneración, delitos informáticos, documentos electrónicos

INTRODUCCIÓN

En la actualidad la mayoría de las personas, sabe que es imprescindible disponer de un sistema de seguridad en la computadora, mínimamente de un antivirus si se está conectado a internet.

Por otro lado es importante considerar la seguridad interna que muchas veces no la consideramos, para ello se debe disponer de herramientas, que permitan el control de acceso a la computadora en las oficinas, donde existen usuarios diferentes trabajando en la misma unidad.

Además en éstas unidades existen técnicos informáticos que apoyan a los funcionarios cuando existe falla en sus computadoras, y como administradores del sistema tienen acceso a la misma, por lo mismo la necesidad de proteger la información.

Word tiene niveles de seguridad para sus documentos, como ser:

- Añadir contraseña a un documento.
- Controlar quien puede abrir, modificar o imprimir un documento.
- Identificar al autor del documento por medio de la firma electrónica
- Proteger el documento contra virus de macros
- Especificar los tipos de cambio que permiten sobre el documento.

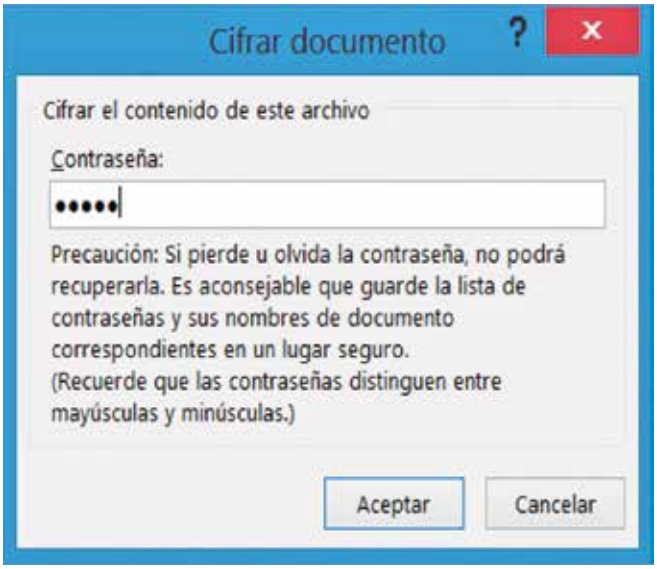
PROBLEMA DE INVESTIGACIÓN

El envío de información confidencial, de un usuario que es el emisor hacia otro usuario que es el receptor, mediante el uso de un canal considerado como inseguro, corre el riesgo de que exista un tercer usuario que este interceptando o recibiendo la información, entonces en muchos de los casos la información enviada puede que ya no sea confidencial.

AÑADIR CONTRASEÑA A UN DOCUMENTO

La contraseña o pasword que se le asigna al documento, puede ser una combinación de caracteres, que pueden contener letras, números, combinación de ambos, mayúsculas minúsculas, para convertir el texto introducido en una cadena de caracteres no descifrables. Para ello se debe acceder a la pestaña Archivo > Información y pulsaremos el botón proteger documentos y elegimos la opción Cifrar con contraseña como se puede ver a continuación:

Figura 1. Cifrado de Documento Word



Fuente: Word 2013

Luego de escribir la contraseña, aparece otro cuadro de dialogo similar, para que se vuelva a escribir la contraseña. Ello permite al sistema asegurar que la contraseña introducida no tuvo errores.

Para modificar la contraseña, se realiza los mismos pasos, y para anular la contraseña solo se borra todo y se deja en blanco.

RESTRICCIONES DE FORMATO Y EDICIÓN

Es otra forma de seguridad para evitar que el documento sea modificado solo en cuanto a formato. Para realizar esta operación se accede a la pestaña Archivo > Información > Proteger documento > Restringir edición, se debe activar la primera opción.

FIRMA DIGITAL

Sirve para asegurar la autoría de un documento, acceder a Pestaña Archivo > Información > Proteger documento > agregar una firma digital al hacer clic siempre que se tenga internet para conectar con la página correspondiente, abre el catálogo de servicios de firmas recomendados por Word, pero para tener la firma digital se debe solicitar con anterioridad a una autoridad certificadora.

El proceso es el mismo para los otros documentos de Office, Excel, PowerPoint.

Aparte de los niveles de seguridad ofrecidos por Word, existen otras aplicaciones, para ocultar o bloquear una carpeta, a continuación se lista un proceso para bloquear una carpeta mediante la creación de un archivo por lotes en un bloc de notas, como se describe a continuación:

```
@ECHO OFF
cls
title Carpeta Confidencial
if EXIST "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" goto UNLOCK
if NOT EXIST Confidencial goto MDLOCKER
:CONFIRM
echo Confirmar antes de bloquear la carpeta(S/N)
set/p "cho=>"
if %cho%==S goto LOCK
if %cho%==s goto LOCK
if %cho%==n goto END
if %cho%==N goto END
echo Elige la opcion correcta.
goto CONFIRM
:LOCK
ren Confidencial "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
attrib +h +s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
echo Carpeta bloqueada
goto End
:UNLOCK
echo Introduce el password para desbloquear la carpeta
set/p "pass=>"
if NOT %pass%== sustituye esta línea roja por tu contraseña goto FAIL
attrib -h -s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
ren "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" Confidencial
echo Carpeta desbloqueada correctamente
goto End
:FAIL
echo El password no coincide... Repite otra vez
goto end
:MDLOCKER
md Confidencial
echo La carpeta Confidencial se ha creado correctamente
```

Luego guarda el archivo como key.bat, hacer doble clic y se crea automáticamente un archivo llamado Confidencial, mover todos los datos a ser protegidos a esa carpeta. Para bloquear hacer doble clic en Key.bat, sale un mensaje de confirmación en la ventana del símbolo del sistema. Digitar S para confirmar, luego la carpeta confidencial se bloqueara y se ocultara. Para acceder al contenido de la carpeta hacer doble clic en el archivo por lotes, inmediatamente pide la contraseña y luego se accede a la carpeta Confidencial.

La protección y la seguridad son muy importantes para mantener la privacidad de los documentos, por eso el establecimiento de contraseñas, pero dichas contraseñas son fácilmente vulneradas por programas que se encuentran en internet, como ser; Advanced Office Password Breaker, Word Password Remover, Word Password Setup, Word Password, Password recovery Pro, Office Password Recovery Toolbox, Office Multi-document Password Cracker, Excel Password Recovery Master, VBA Password Recovery Master, oprlastic. Por ejemplo Advanced Office Password Breaker, recupera la contraseña de un documento Word en pocos minutos, rompe contraseñas y desbloquea los documentos en vez de realizar una recuperación de contraseña larga y pesada.

Desbloquea los documentos Microsoft Word y hojas de cálculo Excel.

Para obtener la contraseña que protege documentos PDF contra copia e impresión se puede utilizar PDFUnlock, unlock-pdf.com, crackmyPDF; funciona subiendo el documento PDF que se encuentra en el disco duro, luego se procede a desbloquear con Unlock.

Elimina las restricciones PDF para copiar, editar, imprimir y extraer. Es Compatible con todas

las versiones de Adobe Acrobat. No requiere instalación de software. Todo se hace en línea. Se seleccione el archivo. Subir Archivo > buscar y seleccionar el archivo PDF que desea desbloquear. Abrir el archivo PDF. Pulse Abrir. Esperar hasta que se abra el PDF. Después de 2 enlaces aparecen desbloqueados y permitirá descargar el PDF con las restricciones eliminadas.

Para abrir archivos .RAR y .ZIP cuando no se conoce la contraseña se puede utilizar; Password Unlocker 3.0, Advanced Archive Password Recovery que funciona como sigue:

Presionar Open para elegir el archivo que se quiere descifrar la contraseña, luego si se piensa que el archivo solo contiene letras, marcar la casilla All caps latin (A-Z) y All small latin (a-z) pero si tuviera números también marcar All digits. Pero si se piensa que la contraseña tiene caracteres especiales marcar All special symbols, cabe hacer notar que cuanto más casillas se marque el tiempo de ejecución será más largo, para la presente investigación se realizó la búsqueda con palabras y dígitos cortos, (ejemplo lui2) la búsqueda tardo aproximadamente 52 minutos, cuando se buscó contraseñas que contenían letras y dígitos de longitud 5, el tiempo fue aproximadamente 2 horas y 23 minutos, en una portátil i7 (se realizó bastantes corridas en diferentes procesadores).

Los métodos que utilizan las herramientas descritas para descifrar los documentos office y PDF, son por fuerza bruta y ataque de diccionario. Fuerza bruta (utiliza el método de prueba y error), prueba todas las letras del abecedario, después sigue con todas las combinaciones de dos letras, luego de tres y así sucesivamente hasta encontrar la palabra que se busca. Ataque de diccionario; es un método de cracking que consiste en intentar averiguar una contraseña probando todas las palabras del diccionario, tiene pocas probabilidades de éxito con sistemas que emplean contraseñas fuertes, con letras mayúsculas y minúsculas mezcladas con números (alfanuméricos) y con cualquier otro tipo de símbolos. Sin embargo, para la mayoría de los usuarios recordar contraseñas tan complejas resulta complicado y generalmente no lo usan, por ende las claves son vulneradas fácilmente.

Las claves o contraseñas, protegen los documentos que se encuentran en nuestra computadora, además actualmente se necesita recordar más contraseñas como ser la tarjeta de crédito, pin de celular, contraseña para el ingreso a las diferentes redes sociales, compras por internet, etc. Por tal razón se utiliza contraseñas sencillas de recordar y se utiliza la misma para todos los casos, sin tener en cuenta lo vulnerables que son.

Cifrar la información es uno de los recursos más eficientes contra muchos de eso ataques, porque, aunque el atacante pudiese eludir cualquier tipo de restricciones de seguridad, si esta convenientemente cifrado lo protegerá de manera segura, de esta manera aunque la información estuviese en manos del atacante, le será inaccesible.

En consecuencia los algoritmos criptográficos no solo garantizan la confidencialidad de la comunicación o del almacenamiento de la información, si no también aseguran la integridad, proporcionando métodos para detectar si un tercero ha manipulado la información

En la actualidad existen algoritmos bastante seguros, basados en cálculos matemáticos, generalmente en la factorización de números primos bastante grandes, lo cual significa que matemáticamente son muy costosos descifrar en tiempo y recursos.

En criptografía se consideran tres elementos básicos:
- Texto en claro
- Clave
- Texto cifrado

El texto en claro puede leerlo cualquier persona. Mediante un algoritmo criptográfico se cifra utilizando una clave. El resultado es el texto cifrado.

Según el tipo de clave se dividen en:

CIFRADO CON CLAVE SECRETA O CRIPTOSISTEMAS SIMÉTRICO

Se tiene una única clave (secreta) que deben compartir emisor y receptor. Con la misma clave se cifra y se descifra, por lo que la seguridad reside sólo en mantener dicha clave en secreto.

CIFRADO CON CLAVE PÚBLICA O CRIPTOSISTEMAS ASIMÉTRICOS

Cada usuario crea un par de claves, una privada para descifrar y otra pública para cifrar, inversas dentro de un cuerpo finito. Lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa. La seguridad del sistema reside en la dificultad computacional de descubrir la clave privada a partir de la pública. Para ello, usan funciones matemáticas de un solo sentido con trampa.

CUERPO DEL TRABAJO

Los datos recolectados, como procesamiento para obtener resultados que apoyen al desarrollo de la presente investigación, se realizó una revisión bibliográfica selectiva sobre el tema objeto de estudio. Se realizó encuestas dirigidos a las Autoridades y Personal Administrativo de la Facultad de Ciencias Puras y Naturales, lo cual permitió recopilar la información necesaria para para el desarrollo del presente Proyecto.

Las encuestas fueron aplicadas a un total de 36 personas entre autoridades y personal administrativo, posteriormente las encuestas fueron tabuladas, el resultado en porcentaje de las mismas es:

Tabla 1. Encuesta a Personal Administrativo sobre manejo de seguridad

1. Sistema Operativo más utilizado:
Linux-Word 8.33%; Word 88.89%; Linux 2.78%.
2. Aplicación más utilizada:
Word-excel-PowerPoint-otro 11.11%; Word-excel-PowerPoint 16.67%; word 13.89%; Word-Excel 19.44%; otro 22.22%; Word-PowerPoint 5.56%; Word-excel-otro 11.11%.
3. Seguridad que utiliza al ingresar a su PC:
Pasword 88.89%; reconocimiento Facial 5.56%; ninguno 5.56%.
4. Seguridad utilizada en documentos Office:
No responde 38.89%; seguridad Word 5.56%; ninguno 55.56%.
5. Quienes tienen acceso a su PC:
Solo Ud. 63.89%; Técnico de la unidad 22.22%; otro (todo el personal) 8.33%; no responde 5.56%.
6. Utiliza métodos de seguridad al enviar documentos por e-mail:
Si 19.44%; no 80.56%.
7. Los documentos que envía vía e-mail sabe si son leídos o interceptados por otras personas:
Si 19.44%; no 77.78%; tal vez 2.78%.
8. Conoces herramientas de seguridad de office:
Si 27.78%; no 72.22%.
9. Utilizas la herramientas de seguridad de office:
Si 16.67%; no 83.33%.
10. Utilizas algún software de seguridad:
Si 19.44%; no 77.78%; no responde 2.78%.

11. Realizas copias de seguridad:

    Disco duro 27.78%; otro dispositivo 47.22%; ambos 8.33%; no responde 11.11%; ninguno 5.56%.

12. El ingreso de contraseña lo hace en secreto:

    Si 80.56%; no 19.44%.

13. Otra persona tiene acceso a su contraseña:

    Si 22.22%; no 77.78%.

14. Su contraseña lo guarda de manera escrita:

    Si 25%; no 91.67%.

15. La contraseña que tiene combina:

    Letras 27.78%; letras y números 52.78%; letras números y caracteres 19.44%.

16. Su contraseña se relaciona con datos familiares:

    Si 33.33%; no 66.67%.

17. Que tan frecuentemente envía información importante o confidencias vía correo:

    Siempre 30.56%; a veces 52.78%; nunca 16.67%.

18. Fue víctima de hackeo:

    Si 33.33%; no 61.11%.

19. Envía correos con varios destinatarios:

    Si 66.67%; no30.56%; a veces 2.78%.

20. Utiliza la misma contraseña para todas sus cuentas de correo electrónico redes sociales y otros:

    Si 27.78%; no 72.22%.

21. Que tan frecuentemente cambia su contraseña:

    Cada mes5.56%; seis meses77.77%; nunca 13.89%; cada año 2.78%.

22. Le gustaría que este protegida la información que usa en su computadora:

    Si 86.11%; no 13.89%.

A continuación se muestra las representaciones gráficas más importantes, que permiten la toma de decisiones del porque se debe proteger la información.

Figura 2. Acceso al equipo

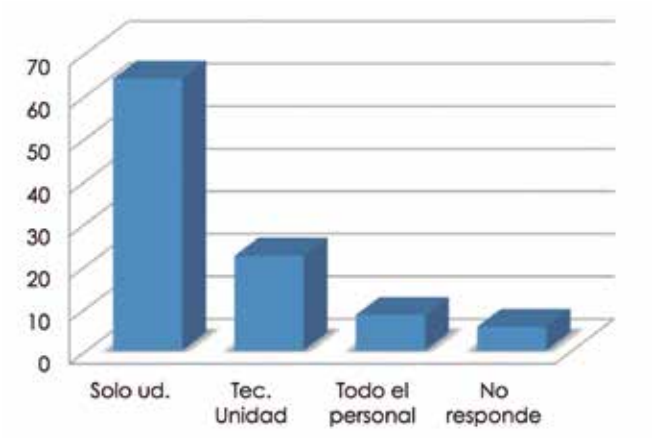


Figura 3. Sistema Operativo utuilizado

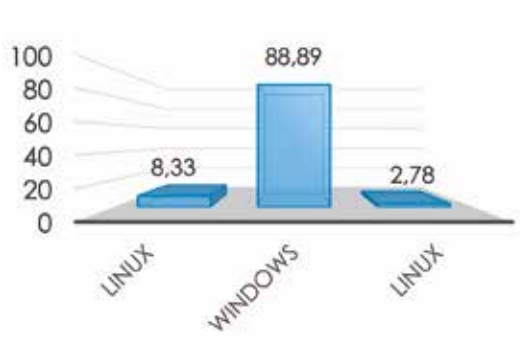


Figura 4. Conoces herramientas de seguridad de office

Figura 5. Seguridad utilizada al enviar por e-mail

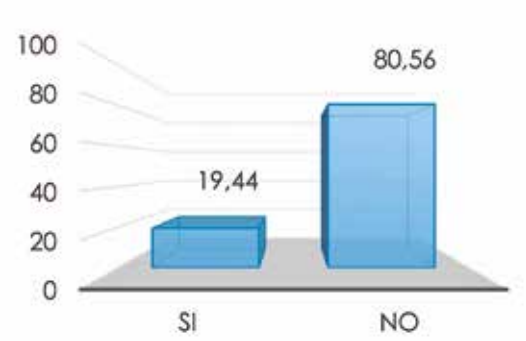


Figura 6. Los documentos via e-mail sabes si es leido

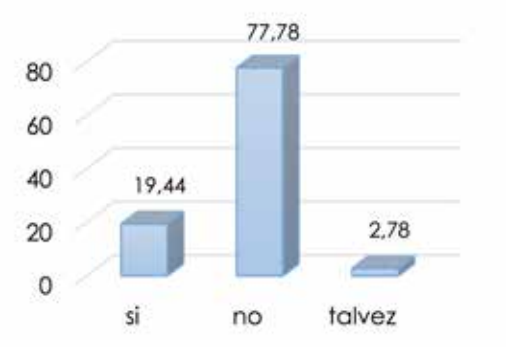
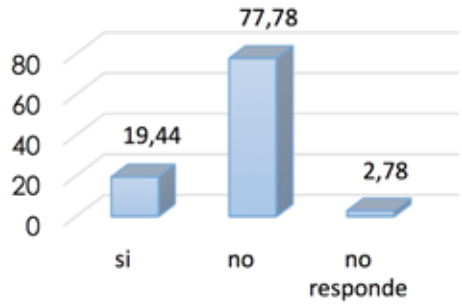


Figura 7. Utilizas algun software de seguridad



De acuerdo al análisis de los resultados de la encuesta, el sistema operativo más utilizado es Windows y Microsoft office y generalmente los documentos enviados vía e-mail, son en formato Word y los mismos son texto plano, además los mismos documentos dentro de su computadora muy pocos usan la seguridad de código que ofrece Microsoft office, también se pudo evidenciar que en un porcentaje, aunque no muy alto el técnico de la unidad tiene acceso a las computadoras, lo cual amerita un riesgo para la vulneración de la información.

CONCLUSIONES Y RECOMENDACIONES

En lo referente a la seguridad Informática, los Bancos y Grupos Financieros de algunos Países del Mundo han tomado en serio el tema de la privacidad de documentos, en nuestro país, particularmente en el área donde se trabajó con las encuestas, no hacen uso de los sistemas de seguridad de Microsoft office como debería ser y menos de herramientas como la criptografía.

Debido al uso masivo de internet, surgen amenazas, como la perdida de privacidad y autenticidad de los documentos electrónicos, si bien la criptografía es una herramienta idónea para la protección de los mismos, es necesario que la legislación penal deba adaptarse a los cambios, a la evolución de la sociedad e incluir un capítulo exclusivo para el tratamiento de las distintas conductas antijurídicas informáticas.

La criptografía permite la transmisión de la información privada mediante un conjunto de técnicas matemáticas, por un canal inseguro, de forma que cualquier intruso que intercepte la comunicación no entienda su significado, por falta de conocimiento de la clave.

RECONOCIMIENTO/AGRADECIMIENTO

Un reconocimiento especial al Instituto de Investigaciones en Informática, por permitir el desarrollo del presente proyecto, al personal administrativo de la Facultad de Ciencias Puras y Naturales, por acceder a brindar toda la información necesaria.

BIBLIOGRAFÍA

- Barragan, J. (2000). Informática y Decisión Jurídica. Mexico: Distribuciones Fontamara.
- Donado, S. A., Zambrana, M. A., & Flechas, A. (2001). Seguridad Computacional. Cauca.
- Garcia, E., López, M. A., & Ortega, J. J. (2005). Una Introducción a la CRIPTOGRAFIA. Castilla.
- Lecoña, Q. &. (2010). CÓDIGO PENAL . La Paz: SIGLA EDITORES.
- Martin, C. V. (s.f.). Privacidad y Protección de Datos Personales en Internet. Mexico.
- Martinez, J. I. (2005). COMPUTACION FORENSE Descubriendo los Rastros Informáticos. Mexico: Alfaomega.
- Neuquen, H. R. (2006). Politica de Privacidad en la Internet. Argentina.
- Onofre, F. O. (2009). PROTECCIÓN DE DATOS PERSONALES ¿Habeas Data o Sistema de Data Protection? Madrid: M.B.
- Tori, C. (2008). HACKING ETICO. Buenos Aires Argentina: Mastroianni Impresiones.
- Ing. Yran Marreno Travieso. Centro Provincial de información de Ciencias Médicas. La Habana.
- Hernando, S, 2005, "Definición de phishing". En: http://www.sahw.com/wp/archivos/26/04/2013/definicion_de_phishing