

# Sistema de generación y cifrado de respaldos de emergencia.

## Trabajo terminal No. 2020-A061

Alumnos: Meza Madrid Raúl Damián\*1, Naranjo Ferrara Guillermo 2

Director: Cortez Duarte Nidia Asunción

\*e-,mail: asdf1234damian@gmail.com

**Resumen** - En el presente documento se plantea el desarrollo de una aplicación que permita, en un caso de emergencia, que el usuario pueda hacer un respaldo diferencial de directorios previamente seleccionados, ya sea por medio de la detección de un patrón de interacción con su celular o a través de una aplicación remota. Este respaldo será cifrado antes de ser enviado a la nube proporcionando seguridad a la información del usuario.

**Palabras clave** - Respaldo, Cifrado, Dispositivos móviles, Nube

## 1. Introducción

En la actualidad, los teléfonos inteligentes se han convertido en un dispositivo fundamental en la vida diaria de las personas, en gran parte gracias a que han tomado el lugar de herramientas de trabajo, cámara digital, medios de entretenimiento y comunicación. Según la ENDUTIH 2019 llevada a cabo por la INEGI, la cantidad de personas que cuentan con un smartphone en México asciende a 72,921,052, de los cuales poco más del 90% cuentan con acceso a internet móvil.[1] Sin embargo, un dispositivo tan utilizado llega a almacenar datos personales de cada propietario, yendo desde contactos, mensajes y toda clase de medios multimedia los cuales llegan a ser más valiosos para el propietario que el dispositivo mismo, hasta, en ocasiones, información más sensible, como es el caso de actividad bancaria, datos biométricos, etc.

Hoy en día, la CDMX se encuentra en una crisis de seguridad, el número de delitos que involucran el despojo de objetos personales como los smartphones incrementa cada año. Sin embargo, se considera que el robo del dispositivo es “*El primer eslabón en una cadena de delincuencia más amplia, ya que muchos de los aparatos robados son usados después para cometer extorsión, secuestros y fraudes*”.[2]

Según Steven Nelson, las copias de respaldo son copias o capturas instantáneas de datos tomadas en un punto particular en el tiempo, almacenadas en un formato global y común, rastreadas durante un periodo de utilidad, y con cada copia subsecuente mantenida de manera independiente de la primera. [3]

Aunque existen diferentes servicios que permiten el respaldo y recuperación de la información de manera periódica así como aquellos que son capaces de eliminar los datos de un dispositivo de manera remota para garantizar que éstos no serán usados por delincuentes, aún existe la necesidad de realizar un respaldo de la información creada antes del robo, la cual pudo no haber sido respaldada hasta el momento y que puede llegar a ser eliminada con el fin de evitar el uso incorrecto de ésta, siendo el caso que no podría recuperarse nunca.

Partiendo de un punto de vista general, la seguridad se define como la cualidad de estar libre de peligro, es decir, protegido ante los adversarios. Ahora bien, en lo que a información se refiere, la seguridad implica brindar protección de ésta con el objetivo de preservar su integridad, confidencialidad y disponibilidad, ya sea que esté almacenada, siendo procesada o transmitida.[4]

Como se ha mencionado, el mantener la información segura, requiere prestar atención a tres servicios esenciales, los cuales [5] define como:

1. Integridad. La información solo puede ser modificada bajo autorización.
2. Confidencialidad. Asegura que el individuo tendrá control e influencia sobre la información relacionada con él será recolectada y guardada, así como por quién será guardada y a quién
3. Disponibilidad. Quienes estén autorizados, pueden acceder a la información.



En este TT se propone el desarrollo de una aplicación para el cifrado de la información contenida en el smartphone, así como la realización de un respaldo en la nube, en caso de presentarse una emergencia involucrando algún delito, haciendo posible que el usuario, por medio de una alerta de emergencia activada con la detección de un patrón de interacción con su smartphone pueda hacer uso de los servicios de seguridad proporcionados por la aplicación.

## Estado del arte

En la tabla 1 se pueden observar algunas de las aplicaciones existentes que tratan con problemáticas similares a la que nuestra aplicación pretende resolver.

SISTEMA	CARACTERÍSTICAS	PRECIO EN EL MERCADO
Privary[6]	<p>Aplicación móvil que permite cifrar fotos, videos y archivos, así como ocultarlos dentro del dispositivo o en tarjeta SD externa. Algunas características son:</p> <ul style="list-style-type: none"> <li>• Cifrado con AES CTR 256 bits.</li> <li>• Respaldo cifrado en la nube.</li> <li>• El usuario selecciona los archivos que desea ocultar y cifrar en el momento.</li> <li>• Camuflar la aplicación y cerrado automático de esta.</li> </ul>	<p>\$24.00 MXN por mes \$250.00 MXN por año \$619.00 MXN de por vida</p>
LockMyPix[7]	<p>Aplicación móvil que oculta y cifra archivos, fotos y video. Algunas características son:</p> <ul style="list-style-type: none"> <li>• Cifrado con AES CTR.</li> <li>• Mantiene la aplicación oculta.</li> <li>• Cerrado automático de la aplicación, opción de cerrarla con movimientos del celular.</li> <li>• Establece PIN falso</li> <li>• Toma de fotografía a intrusos.</li> </ul>	<p>\$30.00 MXN por mes \$119.99 MXN por año \$309.00 MXN de por vida</p>
Caja fuerte de Huawei	Cifra el archivo de texto o multimedia seleccionado y lo mueve a la caja fuerte (una locación oculta) ya sea en la memoria interna o externa del celular.	Incluida como servicio en la compra de un celular Huawei
Encryption Manager[8]	Aplicación móvil para gestión de archivos que permite mantenerlos cifrados. Algunas características son:	\$49.00 MXN
	<ul style="list-style-type: none"> <li>• Cifrado AES y Twofish 128 y 256 bits.</li> <li>• Borrado de archivo original tras ser cifrado.</li> <li>• Copia de seguridad en la nube.</li> </ul>	

Tabla 1. Aplicaciones y Proyectos existentes similares al propuesto en este documento

## 2. Objetivo

Desarrollar una aplicación móvil para celulares Android, que, por medio de un patrón de interacción del usuario con su celular, responda ante una emergencia de robo o asalto, realizando un respaldo cifrado en la nube de la información pre-indicada por el usuario, almacenada en su celular.

### **3. Justificación**

Año tras año se presentan incrementos en los índices delictivos de la CDMX. La Procuraduría General de Justicia de la CDMX reporta que poco más del 60% de los delitos cometidos son delitos contra el patrimonio. [9] Dentro de los delitos contra el patrimonio destacan los delitos a transeúntes con aproximadamente un 18%. Estas cifras representan solamente los delitos denunciados. Según la Asociación Nacional de Telecomunicaciones, tan solo en el 2018 se recibieron 627,920 reportes de robo o extravío de celulares, una cifra tan alta que es alarmante.[10]

Muchas veces, cuando uno de estos delitos es cometido, los usuarios no solo son despojados de un bien económico, sino que, como se describe por Jane Vincent, los usuarios son despojados de “*un repertorio de recuerdos ... fotos y mensajes*”.[11] Gisli Thorsteinsson menciona que, en una encuesta llevada a cabo el 2008 en Nueva Zelanda los usuarios jóvenes entre 18 y 24 años consideran su dispositivo como “*una extensión de sí mismos*”. Así mismo, Vimala Balakrishnan menciona la importancia de las funciones de seguridad de los dispositivos a la hora de que las mujeres de Malasia seleccionar un dispositivo. [12]

Es claro que la importancia de un smartphone se encuentra principalmente en la información que está almacenada, ya que parece más importante para los usuarios recuperar información que recuperar el dispositivo mismo. Actualmente, a la hora de buscar “how to recover a stolen phone”, google logra encontrar 52 mil resultados, mientras que al buscar “how to restore photos”, se encuentran 336 mil resultados.

También existen diferentes razones por las cuales los usuarios no respaldan su información. desde quienes no lo hacen por miedo a que esta pueda ser vista por otras personas, mientras que otros no están dispuestos a pagar por los servicios donde resulta también caro para los proveedores el mantener tanta información almacenada.

Nuestro propósito no es sustituir completamente a los servicios existentes de respaldos en la nube, sino crear un complemento que permita a los usuarios realizar respaldos de emergencia que solamente se mantendrán en la nube durante un tiempo determinado, suficiente para que los usuarios puedan recuperar esta información.

Ya que la mayoría de los sistemas operativos manejan sus archivos por medio de directorios o carpetas, los cuales permiten agrupar los archivos facilitando su acceso a través de nombres de ruta.[15]

Para determinar qué archivos serán respaldados, haremos uso de la estructura de directorios del sistema operativo para identificar los archivos que han sido creados de manera reciente, los cuales se asume no han sido respaldados aun por los otros servicios ya existentes.

#### 4. Productos o Resultados esperados

Nuestro proyecto consistirá de varios módulos los cuales interactúan como se puede ver en la figura 1.

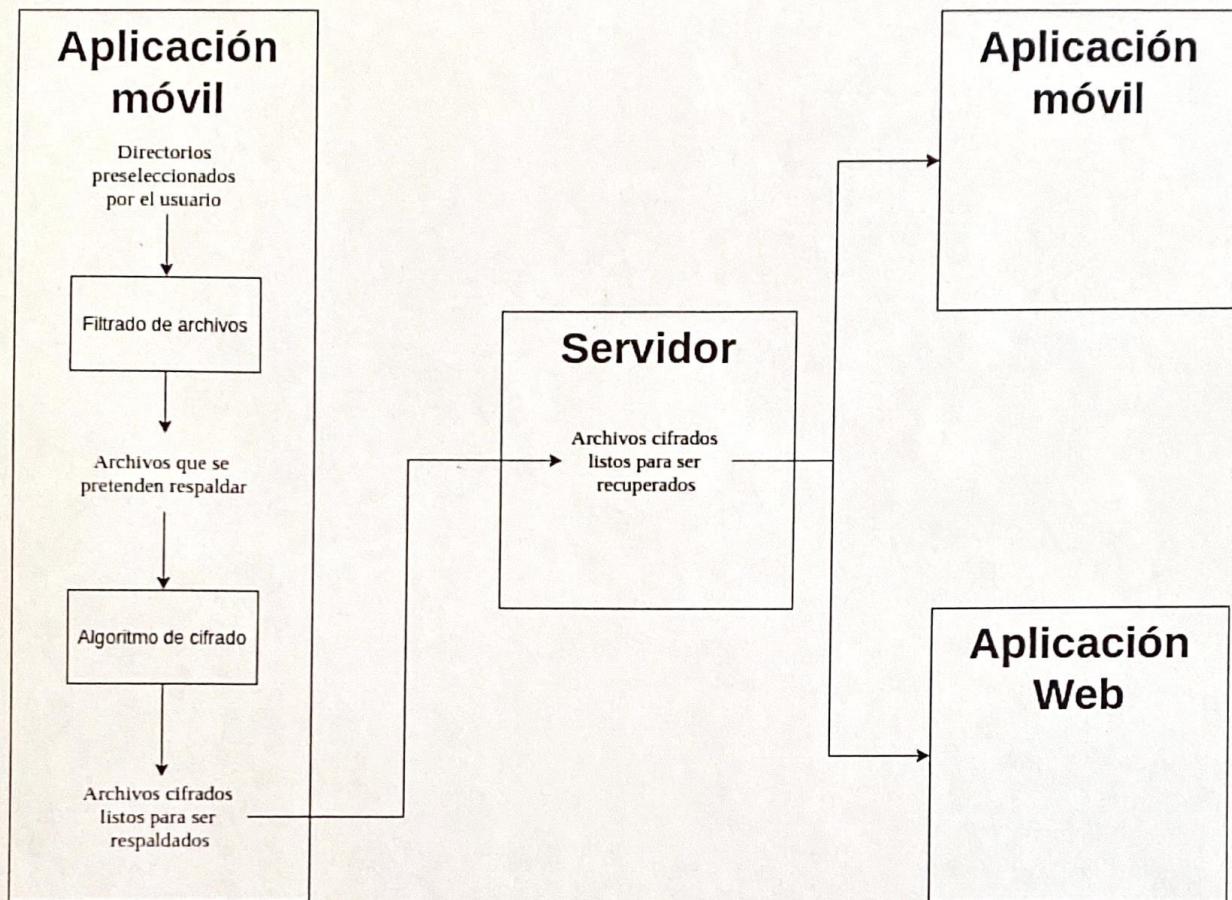


Figura 1. Arquitectura y vista general del sistema

Al finalizar el desarrollo, se pretende contar con los siguientes productos

- Una aplicación móvil que permita a los usuarios cifrar de manera eficiente, haciendo uso de un patrón de interacción entre el usuario y el smartphone, ciertos archivos, respaldarlos y recuperarlos.
- Una aplicación web que permite disparar la rutina de respaldo del celular y posteriormente descargar los datos.
- Manual técnico
- Reporte Técnico

## 5. Metodología

Debido a la evolución del software con el tiempo, es frecuente que los requerimientos del negocio y los productos cambian conforme avanza el desarrollo, por lo mismo es necesario seguir un modelo que se adapte a un producto que evoluciona con el tiempo.[13]

Para este proyecto se a decidido seguir un modelo de procesos evolutivo, usando el modelo o paradigma de prototipos. Este modelo centra el mayor esfuerzo en la creación del prototipo en lugar de concentrarse en la documentación. A su vez, requiere de un mayor involvement del usuario permitiéndole interactuar con el prototipo y así proveyendo retroalimentación, lo que previene de malentendidos y hace más posible que el producto satisfaga al cliente.[14]

Este paradigma comienza con la comunicación entre los participantes (clientes y equipo del proyecto) para definir los objetivos generales del software, identificar los requerimientos y detectar las áreas que es imprescindible que estén bien definidas. Posteriormente se planea una iteración para realizar el prototipo, tras lo cual se lleva a cabo el modelado en forma de un “diseño rápido”, el cual se centra en los aspectos del software que serán visibles a los usuarios. El diseño rápido lleva a la construcción de un prototipo, el cual es entregado y evaluado por los participantes, quienes proporcionan una retroalimentación para mejorar los requerimientos. La iteración ocurre a medida que el prototipo es afinado para satisfacer las necesidades de distintos usuarios.[13]

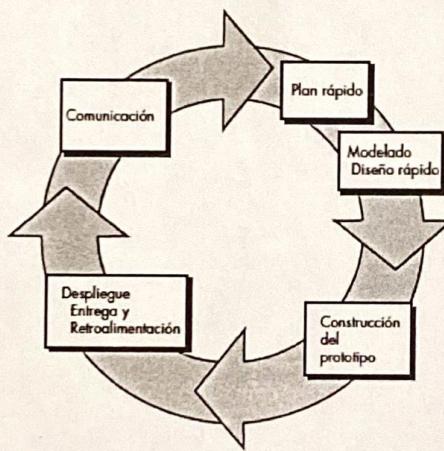


Figura 2. Ciclo de vida del modelo de prototipos [13]

Dos aspectos importantes que cabe señalar, en la elección de este modelo para ser usado son:

1. El prototipo sirve como mecanismo para definir los requerimientos.
2. La gran apertura que da al uso de herramientas o programas ya existentes para generar los prototipos funcionales más rápidamente.

Siguiendo este modelo, se ha decidido realizar 3 prototipos para desarrollo de este sistema, los cuales se describen brevemente a continuación:

- ❖ Prototipo 1. Aplicación móvil que sea capaz de cifrar la información.
- ❖ Prototipo 2. Aplicación móvil capaz de realizar el respaldo de la información en la nube
- ❖ Prototipo 3. Aplicación móvil responda al patrón de interacción del usuario.
- ❖ Prototipo 4. Aplicación web como complemento a la aplicación móvil para recuperar la información.

## 6. Cronogramma

Nombre del alumno(a): Naramio Esteban Guillermo

en el concurso del año inmuno(a), Nahuel Ferrara Guillermo

Nombre del alumno(a): Meza Madrid Raúl Damián  
Título del TT: Sistema de generación y cifrado de m...

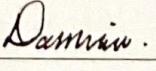
Título del TT: Sistema de generación y cifrado de respaldos de emergencia

## 7. Referencias

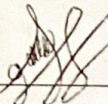
- [1] Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2019, Disponible en: <https://www.inegi.org.mx/programas/dutih/2019/default.html#Tabulados>
- [2] Jonás López, (08/07/2019), Roban más de mil 970 celulares cada día en CDMX, Excelsior, <https://www.excelsior.com.mx/comunidad/roban-mas-de-mil-970-celulares-cada-dia-en-cdmx/1323219>
- [3] Nelson, Steven, and Russell Brown. Pro data backup and recovery. New York: Apress, 2011
- [4] M. E. Whitman, H.J. Mattord, Principles of Information Security 4ta edición. Boston, MA, E.U.A.: Course Technology, 2012.
- [5] W. Stallings, Cryptography and Network Security: Principles and Practice 6ta edición. Estados Unidos: Pearson, 2014.
- [6] fourchars. (2020). Privary (2.6.22 (Lancelot)). [Aplicación Móvil]. Play Store. [https://play.google.com/store/apps/details?id=com.fourchars.privary&hl=es\\_MX](https://play.google.com/store/apps/details?id=com.fourchars.privary&hl=es_MX)
- [7] fourchars. (2020). LockMyPix (4.2.4 (Gemini)). [Aplicación Móvil]. Play Store. [https://play.google.com/store/apps/details?id=com.fourchars.lmpfree&hl=es\\_MX](https://play.google.com/store/apps/details?id=com.fourchars.lmpfree&hl=es_MX)
- [8] giraone. (2017). Encryption Manager (4.5.4). [Aplicación Móvil]. Play Store. [https://play.google.com/store/apps/details?id=com.giraone.encmanfull&hl=es\\_MX](https://play.google.com/store/apps/details?id=com.giraone.encmanfull&hl=es_MX)
- [9] Boletín estadístico de la incidencia delictiva en la ciudad de méxico 2019, Disponible en: <https://www.fgjcdmx.gob.mx/storage/app/media/Esta./2019/boletin-2019.pdf>
- [10] Asociación Nacional de Telecomunicaciones, Programa de seguridad, Disponible en: <http://www.anatel.org.mx/programaseguridad.php>
- [11] Vincent, J. Emotional attachment and mobile phones. *Know Techn Pol* 19, 39–44 (2006). Disponible en: <https://doi.org/10.1007/s12130-006-1013-7>
- [12] Thorsteinsson, G., and Page, T., 2014. User attachment to smartphones and design guidelines. *International Journal of Mobile Learning and Organization*, 8 (3), pp. 201 - 215
- [13] R.S Pressman, Ingeniería de Software. Un enfoque práctico 7ma edición. Nueva York, E.U.A.: McGrawHill, 2010.
- [14] R. G. Sabale, y A. R. Dani, “Comparative study of prototype model for software engineering with system development life cycle”, *IOSR Journal of Engineering (IOSRJEN)*, vol. 2, pp. 21-24, 2012.
- [15] Tanenbaum, Andrew S. Modern operating systems. Upper Saddle River, N.J: Pearson Prentice Hall, 2008

## 8. Alumnos y directores

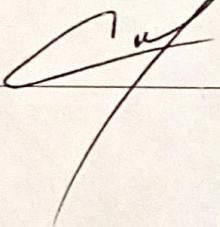
*Meza Madrid Raúl Damián.*.- Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta: 2017631051, Teléfono: 55 1639 1630, email: damianmezamadrid@gmail.com..

Firma: 

*Naranjo Ferrara Guillermo.*.- Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Espacialidad Sistemas, Boleta: 2014140514, Teléfono: 55 1939 2011, email: memonaranjof@gmail.com.

Firma: 

*Cortez Duarte Nidia Asunción.*.- Maestra en Ciencias en Computación CINVESTAV-IPN 2009, Ing. en Sistemas Computacionales ESCOM-IPN 2006, Profesora en ESCOM Depto. de Ingeniería en Sistemas Computacionales. Áreas de interés: criptografía, seguridad de información, hardware reconfigurable, aritmética computacional, diseño digital. Teléfono: 57-29-6000 ext. 52032, nidiacortez3@gmail.com.

Firma: 

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.