UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

TESIS DE GRADO

“CONTROL Y SEGURIDAD DE LOS EMPLEADOS ANTE AMENAZAS INFORMÁTICAS EN DISPOSITIVOS MÓVILES”

PARA OPTAR AL TÍTULO DE LICENCIATURA EN INFORMÁTICA
MENCIÓN: INGENIERÍA DE SISTEMAS INFORMÁTICOS

POSTULANTE: EDWIN GONZALO MAMANI LIMACHI

TUTOR METODOLÓGICO: M.Sc. FRANZ CUEVAS QUIROZ

ASESOR: Lic. JUAN GONZALO CONTRERAS CANDIA

NUESTRA SEÑORA DE LA PAZ –BOLIVIA

2017

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

LA CARRERA DE INFORMÁTICA DE LA FACULTAD DE CIENCIAS PURAS Y NATURALES PERTENECIENTE A LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) visualizar el documento mediante el uso de un ordenador o dispositivo móvil.

b) copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.

c) copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la referencia correspondiente respetando normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

Dedicatoria

Con todo mi amor y cariño para mis padres Emilio y Andrea que me brindan toda la fortaleza para que mi persona pueda lograr los sueños en vida, por motivarme y darme la mano y su apoyo en todo momento, a ustedes por siempre mi corazón y mi agradecimiento.

AGRADECIMIENTO

A Dios por darme fortaleza en los tiempos más difíciles y guiarme en el camino de la vida.

A mi Tutor Metodológico M.Sc. Franz Cuevas Quiroz por su apoyo, enseñanzas, colaboración predisposición y comprensión que lo caracterizan.

A mi Revisor Lic. Juan Gonzalo Contreras Candia por haberme guiado en la elaboración y desarrollo de la presente Tesis de Grado, con sus consejos y su amistad.

Agradecer a todos los docentes, compañeros de la carrera de Informática y a la Universidad Mayor de San Andrés por ayudarme en mi formación como profesional.

A todos ellos muchas gracias.

RESUMEN

El control y seguridad de los empleados ante amenazas informáticas en dispositivos moviles, está tomando una gran importancia en el presente para cualquier organización que maneje información importante que incluyan las actividades de sus empleados.

En la presente mantener la seguridad es el objetivo a lo que más se deben enfocar las organizaciones, el interés y la demanda de aplicaciones para teléfonos móviles y tablets que cada vez se asemejan más a ordenadores portátiles por la capacidad que estos tienen y las tareas que estos pueden llegar a desempeñar, crece rápidamente, el cual impulsa rápidamente a los usuarios a interactuar con el dispositivo en cualquier momento del día ya sea en el trabajo o en su casa, incrementando también las amenazas informáticas.

La herramienta propuesta para ese problema es un prototipo aplicación Android que permita el control y seguimiento de las actividades de un empleado que tiene a cargo un dispositivo móvil perteneciente a una organización, con el fin de mantener informado a los responsables de la organización ante posibles amenazas o fugas de información por causa de los empleados.

En desarrollo del prototipo se implementó métodos de encriptación hibrida para resguardar la información generada por el empleado, se trabajó en la plataforma de Android Studio el cual implementa lenguaje Java y XML para su desarrollo.

Se realizaron tres pruebas en distintos casos que el empleado pudo haber manipulado el dispositivo móvil, los resultados obtenidos son satisfactorios y alcanzan un valor aceptable los cuales son registrados en reportes para un mayor análisis de las posibles amenazas informáticas los cuales son considerados como factores de riesgo que determinan un porcentaje de que podría aquejar a cualquier organización.

ABSTRACT

The control and security of employees against computer threats in mobile devices is taking on great importance in the present for any organization that handles important information that includes the activities of its employees.

In the present maintain security is the objective to which most organizations should focus, the interest and demand for applications for mobile phones and tablets that increasingly resemble laptops by the capacity they have and the tasks that These can play, grows rapidly, which quickly encourages users to interact with the device at any time of the day either at work or at home, also increasing computer threats.

The proposed tool for this problem is a prototype Android application that allows the control and monitoring of the activities of an employee who is in charge of a mobile device belonging to an organization, in order to keep those responsible for the organization informed of possible threats or information leaks because of employees.

In the development of the prototype, hybrid encryption methods were implemented to safeguard the information generated by the employee. We worked on the Android Studio platform, which implements Java and XML language for its development.

Three tests were performed in different cases that the employee could have manipulated the mobile device, the results obtained are satisfactory and reach an acceptable value which are recorded in reports for a greater analysis of the possible computer threats which are considered as risk factors that determine a percentage that could affect any organization.

ÍNDICE

Pág.

ÍNDICE DE FIGURA

ÍNDICE DE PROGRAMAS

CAPITULO I

INTRODUCCIÓN

El control y la seguridad de los empleados ante amenazas informáticas en dispositivos móviles son necesarias por parte de las organizaciones públicas y privadas ya que están expuestas a sufrir robos de información, mal uso de los dispositivos móviles llegando a ser un problema de la organización.

"Los criminales de ahora están haciendo uso de la tecnología para facilitar su ofensiva sobre todo a los bancos, obtener información de ciertas personas dentro de las compañías con el fin de chantajearlas u obtener información confidencial de una empresa para luego traficar con estas. Pero estos crímenes no son casuales, ya sea esta por un empleado de la empresa que esta con malas intenciones o ya sea por supuestos "hackers", la información digital tiene mucho valor cuando se sabe cómo explotarla, como resultado de estas se oyen noticias acerca de drogas, pornografía, cuantas bancarias vacías, empleados implicados, chantajes, vidas privadas reveladas en la web, incluso actos terroristas, en fin, muchos actos ilegales que difícilmente pueden ser probados ante la justicia cuando no se tiene evidencia de los mismos" (Casey, 2004).

Todo este avance informático también genera un grado de crimen que crece a un ritmo preocupante a las organizaciones que cuentan y tienen a cargo una gran cantidad de información, que generan ingresos a estos, estos crímenes se pueden encontrar tanto en las organizaciones como fuera de ellas.

"La tensión entre seguridad y productividad de la empresa nunca ha sido tan aguda. Para que funcionen al máximo rendimiento y con la máxima competitividad, las organizaciones necesitan que sus empleados tengan acceso a los recursos de la empresa desde cualquier lugar y de más formas que antes pero la proliferación de distintos lugares de trabajo, distintos tipos de trabajadores y diferentes métodos de acceso ha empujado las estrategias de seguridad tradicionales a un punto de ruptura. La consumerización de las TI añade una gran complejidad al entrar en liza en el entorno una mezcla diversa de portátiles, tabletas y smartphones, dispositivos, unos provisionados por la empresa y otros propiedad del personal. La diversidad de los dispositivos ha dado lugar a un alto grado de complejidad, ya que las múltiples combinaciones de sistemas operativos, aplicaciones y configuraciones han destruido la coherencia del modelo de gestión del ordenador portátil empresarial" (Citrix, 2013).

La presente tesis plantea el desarrollo y construcción de un prototipo una aplicación Android, con la aparición de las computadoras, la información que estas podían contener almacenadas, permitió al usuario interactuar diariamente con el fin de automatizar muchos de los procesos repetitivos de las tareas manuales en el trabajo que se realizan como en organizaciones, fundaciones, empresas públicas o privadas u otras. Mientras que los ordenadores incrementaban su capacidad también incrementaba la información almacenada a tal punto que en la actualidad la información es muy importante.

1.1. ANTECEDENTES

En nuestro país en el presente se está implementando en las empresas, organizaciones e instituciones del gobierno el uso de los dispositivos móviles inteligentes como ser celulares o tablets como un activo de la institución ya sea para el registro de productos o llamadas a la entidad y coordinación con los empleados del trabajo que realizan para estas organizaciones como un instrumento indispensable cotidiano.

En cuanto a las leyes de un país relacionado al software, la privacidad y la seguridad determina un papel importante dentro de las políticas de seguridad de una organización. En nuestro país de acuerdo al Decreto Supremo Nº 1793, 13 de noviembre de 2013 que hace referencia en el artículo 3 inciso VI Respecto a la seguridad informática.

a) Seguridad informática: Es el conjunto de normas, procedimientos y herramientas, las cuales se enfocan en la protección de la infraestructura computacional y todo lo relacionado con ésta y, especialmente, la información contenida o circulante.

b) Seguridad de la información: La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

Por otra parte OECD Information Security and Privacy, es una organización internacional que trata de crear guías para la protección de la privacidad y el tráfico de información personal a nivel mundial, tomando en cuenta las distintas leyes de cada país, fomentado hábitos y prácticas comunes.

Los trabajos relacionados con la presente tesis son:

La tesis de pregrado "*MONITOREO DE AMENAZAS INFORMATICAS PARA EL CONTROL DE SEGURIDAD DE LOS EMPLEADOS*", de William Kenny Pocho Challco (2009), Universidad Mayor de San Andrés, La Paz, Bolivia. Su propósito es: Vulnerabilidad de las amenazas informáticas en alguna organización por parte de los empleados que tienen acceso a información del área de trabajo.

La tesis de pregrado "*COMPARACION Y EVALUACION DE ALGORITMOS DE INCRIPTACION ASIMETRICA Y FIRMAS DIGITALES*", de Gustavo Andrés Flores Alconini (2010), Universidad Mayor de San Andrés, La Paz, Bolivia. Su propósito es: Criptología la cual tiene diversas líneas de investigación, entre los cuales se menciona la Criptología Cantica, criptografía de curvas hiperelipticas, criptografía por hardware, entre otros.

La tesis de pregrado "*SEGURIDAD EN TRANSACCIONES EN LINEA CON TARJETA*

DE DEBITO MEDIANTE METODOS DE ENCRIPTACION ASIMETRICA HIBRIDA", de Arturo Ricardo Mirabal Alvarado (2010), Universidad Mayor de San Andrés, La Paz, Bolivia. Su propósito es: Criptografía sobre el uso de tarjetas bancarias, pero se hace referencia a criptografía hibrida y criptografía tradicional.

1.2. PLANTEAMIENTO DEL PROBLEMA

"Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores" (Mitnick, 2008).

En la actualidad mantener la seguridad es el objetivo a lo que más se deben enfocar las organizaciones, el interés y la demanda de aplicaciones para teléfonos móviles y tablets que cada vez se asemejan más a ordenadores portátiles por la capacidad que estos tienen y las tareas que estos pueden llegar a desempeñar, crece rápidamente, el cual impulsa rápidamente a los usuarios a interactuar con el dispositivo en cualquier momento del día ya sea en el trabajo o en su casa, incrementando también las amenazas informáticas.

Debido a esta expansión tecnológica, la seguridad de la información se puede volver más vulnerable sino se toma las debidas precauciones por parte de las organizaciones, a continuación, se mencionan algunas:

- Algunos empleados buscan distracción con los dispositivos móviles el cual tiene unos resultados desfavorables para la organización.
- Una copia de alguna información importante que se encuentra en el dispositivo móvil del empleado.
- El borrado de la información, dejar de guardar los datos por falta de responsabilidad con el móvil.
- Perdida del móvil, perdida del informe de los trabajos realizados por el empleado, daños económicos a la organización.

En consecuencia se plantea el siguiente problema de investigación:

¿Una aplicación Informática realizara el control y la seguridad de la información de los dispositivos móviles que usan los empleados, en el cual las organizaciones están expuestas ante posibles amenazas informáticas?

1.3. OBJETIVOS

1.3.1 OBJETIVO GENERAL

Desarrollar una aplicación Android que permita el control y seguimiento de las actividades de un empleado que tiene a cargo un dispositivo móvil perteneciente a una organización, con el fin de mantener informado a los responsables de la organización ante posibles amenazas o fugas de información por causa de los empleados.

1.3.2 OBJETIVOS ESPECÍFICOS

Con el fin de dar solución al problema planteado se presenta los siguientes objetivos específicos:

- Diseñar el módulo de monitoreo de las actividades de un empleado respecto al movimiento de la información digital dentro de una organización, ya que esta es abundante y dentro de la cual existe transacciones financieras y otro tipo de información que fácilmente son difundidos.
- Encriptar la información recolectada con el algoritmo de encriptación AES y RSA.
- Implementar análisis de búsqueda de la información recolectada, para encontrar indicios concretos que puedan ser consideradas esenciales como evidencia cuando la organización sufra una pérdida o divulgación de la información por causa de un empleado
- Documentar la información que los empleados han manipulado en los dispositivos móviles de la organización, para su posterior uso en reportes detallados.

1.4. HIPÓTESIS

"La aplicación *Control y Seguridad de los Empleados ante amenazas Informáticas en Dispositivos Móviles* almacena las actividades realizadas en el dispositivo móvil de manera eficaz para luego ser analizadas y estar prevenidos ante amenazas informáticas."

1.5. JUSTIFICACIÓN

La propuesta de esta tesis es una herramienta, implementando algoritmos de encriptación, captura de teclado en pantalla, desarrollada en el lenguaje de programación Android y bajo el sistema operativo Android, la cual podrá ser utilizada por una organización.

Es muy importante el avance científico en los dispositivos móviles facilitando el trabajo de las organizaciones, el intercambio de información del trabajador con el dispositivo móvil el cual brinda a los clientes o usuarios de los productos o actividades de la organización, con esta razón fueron necesarios crear los protocolos de seguridad para proteger el flujo de información.

Por tanto, el desarrollo de esta aplicación se justifica porque constituye en una herramienta informática diferente en el área de control de empleados en las organizaciones.

1.6. ALCANCES Y LÍMITES

Se va desarrollar una aplicación Android que capture las acciones de un empleado sobre un dispositivo móvil, mientras esté trabajando en el mismo. Al mencionar la captura de las acciones del usuario, se está refiriendo a lo que está tecleando en la pantalla del dispositivo móvil, si el empleado está cumpliendo con las actividades de la organización, o en tal caso que esté realizando actividades personales: ya sea chateando, viendo videos, escuchando música, jugando, etcétera. Toda la información recolectada se ira guardando en archivos encriptados, para luego proveer indicios de malintencionados, robo de información, entre otros.

La aplicación tendrá un respaldo de información, el cual nos permita un backup remoto en un servidor externo a la organización, en caso de falla del sistema operativo, formateo del dispositivo móvil, etcétera. En cuanto a los límites y alcances.

- La aplicación Android se instalará en dispositivos móviles donde se crea que pueda existir fuga de información.
- La aplicación Android no se ejecuta cuando el Sistema Operativo se inicie en modo a prueba de fallos.

Este trabajo está enfocado a los dispositivos móviles inteligentes con sistemas operativo Android porque es el sistema operativo predominante en el mercado de los celulares y tablets.

CAPITULO II

MARCO TEÓRICO

2.1 DISPOSITIVO MOVIL

"Los terminales constituyen en el elemento clave para el éxito de las nuevas redes móviles 3G, es decir aquellas redes que vinculan la posibilidad de transferir datos en movimiento. Los terminales son el único elemento de toda la compleja cadena de las nuevas redes que ve el usuario, y como tal, tiene una importancia trascendental para la percepción final de la calidad de los servicios y redes" (Vásquez, 2008).

Un dispositivo móvil se puede definir como un aparato de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, que ha sido diseñado específicamente para una función, pero que puede llevar a cabo otras funciones más generales.

2.1.1 ANDROID

Android es una plataforma de desarrollo libre, y de código abierto: El núcleo del sistema está basado en un Linux (versión 2.6 para versiones anteriores a Android 4.0 Ice Cream Sándwich y versión 3.0 del kernel para posteriores) al que se le han hecho ciertas modificaciones para que pueda ejecutarse en teléfonos y terminales móviles. Las

modificaciones se han realizado para adaptarlo a los menores recursos de los dispositivos móviles, que aunque cada vez son más potentes, no dejan de tener menos recursos que un ordenador de sobremesa.

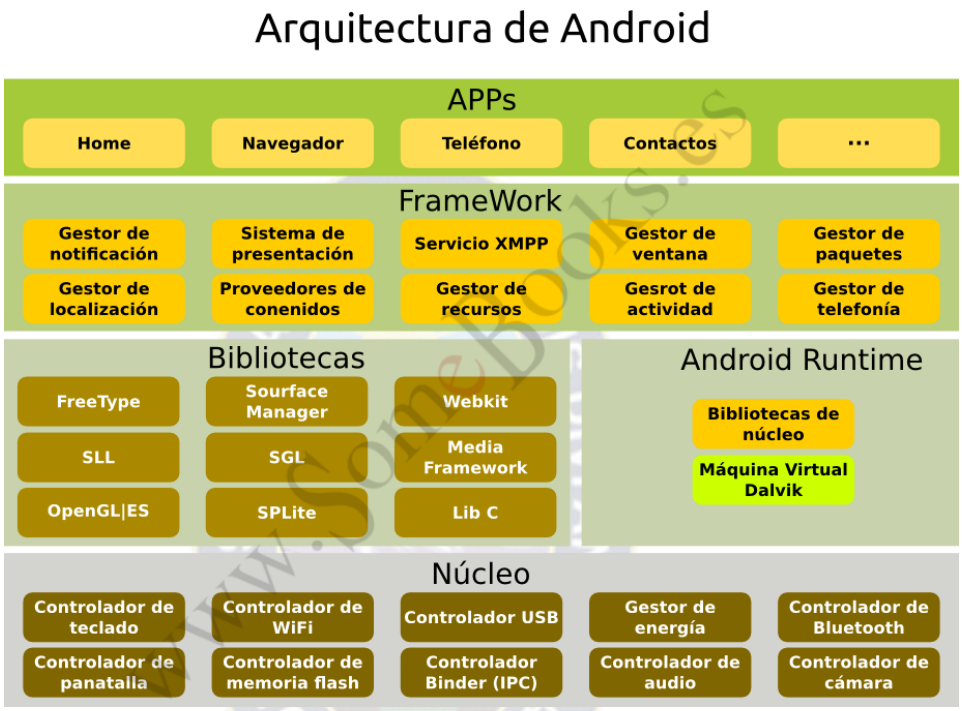


Figura 2. 1: Arquitectura de Android
Fuente: somebooks.es, 2017

2.1.2 LENGUAJE JAVA

Java es un lenguaje de programación y una plataforma informática comercializada por primera vez en 1995 por Sun Microsystems. Hay muchas aplicaciones y sitios web que no funcionarán a menos que tenga Java instalado y cada día se crean más. Java es rápido, seguro y fiable. Desde portátiles hasta centros de datos, desde consolas para juegos hasta súper computadoras, desde teléfonos móviles hasta Internet, Java está en todas partes.

2.2 CONTROL Y SEGURIDAD

"El control ha sido definido bajo dos grandes perspectivas, una perspectiva limitada y una perspectiva amplia. Desde la perspectiva limitada, el control se concibe como la verificación a posteriori de los resultados conseguidos en el seguimiento de los objetivos

planteados y el control de gastos invertido en el proceso realizado por los niveles directivos donde la estandarización en términos cuantitativos, forma parte central de la acción de control. Bajo la perspectiva amplia, el control es concebido como una actividad no sólo a nivel directivo, sino de todos los niveles y miembros de la entidad, orientando a la organización hacia el cumplimiento de los objetivos propuestos bajo mecanismos de medición cualitativos y cuantitativos. Este enfoque hace énfasis en los factores sociales y culturales presentes en el contexto institucional ya que parte del principio que es el propio comportamiento individual quien define en última instancia la eficacia de los métodos de control elegidos en la dinámica de gestión. Todo esto lleva a pensar que el control es un mecanismo que permite corregir desviaciones a través de indicadores cualitativos y cuantitativos dentro de un contexto social amplio, a fin de lograr el cumplimiento de los objetivos claves para el éxito organizacional, es decir, el control se entiende no como un proceso netamente técnico de seguimiento, sino también como un proceso informal donde se evalúan factores culturales, organizativos, humanos y grupales. ” (Cabrera, 2003).

“La seguridad como un derecho, una necesidad humana y una función del sistema jurídico. Hace énfasis en los delitos contra la propiedad: robo y hurto. Está íntimamente relacionado con la construcción social del miedo”. (Ávila, 2006)

2.2.1 CYBER-CRIMEN

“Un cyber-crimen ocurre cuando la información digital es utilizada para cometer o encubrir un agravio, lo cual incluye: fraude financiero, sabotaje de datos o de la red, robo de información personal, penetración de un sistema o negación de un servicio, acceso no autorizado de empleados o miembros de una organización al acceso de la Internet con ciertos privilegios, virus que pueden brindar amenazas a través de la Internet. Un cyber-crimen puede ser catalogado como un evento interno o externo. Típicamente las grandes amenazas a la organización ha sido empleados y personal de confianza, lo cual es ¿Por qué un crimen de computadora esta frecuentemente referido como un crimen de un miembro de la organización?. En cambio un cyber-crimen, como un evento externo, es difícil de predecir ya que este ataque no tiene ningún motivo en contra de la organización**”** (Vacca, 2002).

2.2.2 CRITERIOS DE INFORMACION

"Para evaluar la información existen varios criterios que debes conocer. Estos son: Relevancia, Alcance, Autoridad-Credibilidad, Actualidad y Objetividad y Exactitud. Una breve explicación de cada criterio se presenta a continuación:

Relevancia es un elemento basado en el juicio. Usualmente para establecer la relevancia debes determinar qué información necesitas, que tipo de fuentes vas a utilizar y cómo utilizarás la información (ensayo, monografía, presentación). Es importante determinar la relevancia en torno al tema que estas investigando.

Alcance para conocer si el documento que has seleccionado tiene el alcance adecuado, debes examinar el contenido de la información si tiene un balance entre los datos y las opiniones. Como marco de comparación debes consultar otras fuentes que presenten otros puntos de vistas a favor y en contra del tema. Esto te ayudara a enfocar tu proyecto desde varias perspectivas.

Autoridad / Credibilidad para determinar la autoridad de la fuente se toma en consideración varios aspectos. Al comparar un documento de una base de datos versus un documento que aparece en la Internet, se puede inferir que los documentos contenidos en las bases de datos incluyen elementos esenciales tales como: nombre del autor, el título de la publicación y más. Por otro lado, en la Internet muchas veces los documentos no presentan estos datos esenciales. En cambio, los documentos que aparecen en las bases de datos, pasan por un proceso de revisión ya que está en juego la reputación de la empresa, mientras que los documentos publicados en la Internet no tienen ningún mecanismo de control de calidad y cualquier persona puede publicar en este medio sin tener experiencia o peritaje en el tema" (Figueroa, 2007).

2.2.3 HARDENING

"Proceso e endurecimiento o aseguramiento de los equipos, principales los servidores. Revisión en busca de las formas más comunes de compromiso que puede tener un posible destino de ataques" (Horna 2007).

Hardening (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc.; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso además de muchas otros métodos y técnicas.

Figura 2. 2: Sistema Hardening
Fuente: userscontent2.emaze.com, 2017

2.2.4 MONITOREO

"El monitoreo y la evaluación significa recoger y usar información. Mientras que en la mayoría de los aspectos de nuestras vidas se reconoce la importancia de la información, en el contexto de proyectos y organizaciones no se reconoce la importancia de la información obtenida del monitoreo y evaluación. Con frecuencia, en el campo del desarrollo, el monitoreo es un requisito impuesto por los donantes en las instituciones. Como tal, los que reciben financiamiento son renuentes a realizar las actividades de monitoreo requeridas. El monitoreo también es visto como un fin en sí mismo, por lo que algunos gerentes de proyecto completan formularios y preparan informes sin que necesariamente utilicen la información para la evaluación interna y planificación del programa" (Handbook, 1997).

2.3 MONITOREO DEL MOVIMIENTO DE LA INFORMACIÓN DIGITAL

"Monitoreo del tráfico de la red en tiempo real con atributos convenientemente de actividades online a una individual y localizar otros blancos. Muchas organizaciones usan sistemas de detección de intrusión para monitorear continuamente al tráfico de la red, puede ser deseable limitar la cantidad y el tipo de información que es recolectada. Por ejemplo, los investigadores digitales únicamente están autorizados para monitorear el tráfico Web. Por lo tanto, recolectar primero, filtrar y analizar después cuando sea posible, y estar seguro que tú sabes que suposiciones estas herramientas están realizando antes de limitar la recolección. Cuando es necesario filtrar, capturar cualquier cosa y solamente excluir lo que no es requerido" (Casey, 2004).

a) MOVIMIENTO DE LA INFORMACIÓN

"Esencialmente es la combinación de números que representan información de varios tipos, incluyendo texto, imágenes, audio, y video. Tomemos un momento para considerar los tipos de datos digitales data que existen y como éstos pueden ser útiles en una investigación. Las computadoras son ubicuos (omnipresentes) y los datos digitales están siendo transmitidos a través del aire alrededor de nosotros y a través de cables en la tierra debajo de nuestros pies" (Casey, 2004).

b) DIGITAL

"Representación de la información usando números. La representación de la información usando dígitos binarios (bits) y valores hexadecimales son casos especiales de un representación digital" (Casey, 2004).

2.4 SEGURIDAD DE LA INFORMACIÓN

"En la actualidad las empresas, de cualquier tipo y sector de actividades, se enfrentan cada vez más con riesgos e inseguridades (ya sean físicos o lógicos) de diversas procedencias que pueden dañar de forma importante sus sistemas de información: Riesgos físicos: Incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados, etcétera. Riesgos lógicos: Fraudes informáticos, espionaje, virus, ataques de intrusión, denegación de

servicios, etcétera. La seguridad no es un producto sino un proceso. La información en realidad está en diversos medios de almacenamiento, impresos, digitales, el conocimiento de las personas. La información en realidad está en diversos medios de almacenamiento de almacenamiento, impresos, digitales, el conocimiento de las personas. Los problemas de seguridad pueden implicar: Alteración de datos, eliminación de datos, publicaciones no autorizadas, Descubrir información reservada. Los usuarios son uno de los puntos más comunes a la hora de comprometer la seguridad un sistema. Es importante concientizar y hacer parte del sistema al usuario" (Horna, 2007).

2.4.1 GESTIONAR

"Dentro del objeto de la administración y gerencia del conocimiento está lo que la empresa sabe sobre sus productos, procesos, mercados, clientes, empleados, etcétera, y sobre el cómo combinar estos elementos para hacer a una empresa competitiva. En este aspecto, esta disciplina parece replicar al objetivo de la Gestión Tecnológica, pero por ser de mayor alcance parece contenerla. Cuando se describe la gestión tecnológica, normalmente se mencionan algunas actividades tales como: Prospección – Selección – Negociación – Adquisición – Adaptación – Modificación – Generación (Innovación)" (Zorrilla, 2016).

2.4.2 GESTIÓN EFICIENTE DE LA ACCESIBILIDAD DE LA INFORMACIÓN

"El exceso de información se convierte a menudo en un problema tan importante como la carencia de la misma, y ello se pone de manifiesto en cualquier proyecto relacionado con infraestructura de almacenamiento y provisión de capacidad. A menudo, una vez que los sistemas entran en producción, se constata que el espacio asignado a un determinado aplicativo ya se ha quedado corto. Llegando a este punto, la única solución es ampliar infraestructura (comprar más disco, ampliar las cabinas, conmutadores SAN, etcétera), o lo que es lo mismo, incrementar el presupuesto asignado. La forma más eficiente de gestionar todo lo anterior es una estrategia conocida como ILM (Information Lifecycle Management), en la que la implantación de una arquitectura hardware/software concreta es la última de las fases, una vez conocidas las necesidades y perfil de la información manejada por el cliente. ILM es una estrategia de TI que se basa en premisas tales como que la información no se genera de la misma manera, no tiene la misma importancia y ésta varía con el tiempo, de

forma que en cada momento requiere niveles de accesibilidad y protección. Para cada tipo de Información de acceso más frecuente: cabinas de discos de alto rendimiento. Información que debe ser retenida durante meses de forma confidencial: soluciones de archivos, cifrado y gestión documental. Información que debe ser salvaguardada durante meses o años: librerías de cintas. Todo ello gestionado mediante herramientas software que proporcionan un paraguas desde dónde gestionar de forma integral toda la infraestructura, así como el movimiento de datos entre la misma" (Martínez, 2008).

2.5 ENCRIPTAR

"Encriptar es ocultar el significado de un mensaje, para que éste no pueda ser leído. Esto conlleva al término de la Criptografía, la cual es usada para mezclar el contenido de un archivo o mensaje para que éste no pueda ser leído de manera clara. La palabra criptografía viene del Griego 'kripto', el cual significa 'ocultar' y 'graphien', el cual significa 'escribir'" (Solomon, Barrett y Broom 2005).

a) ENCRIPTAR INFORMACION

"Las prácticas comunes de la encriptación de la información en general nos proveerá: Confidencialidad que nos asegura que únicamente los usuarios autorizados puedan ver el mensaje, Integridad que nos asegura que únicamente los usuarios autorizados pueden cambiar o modificar el mensaje. Autentificación que nos asegura que los usuarios son quienes dicen ser, No Repudiación que nos asegura que un mensaje se originó desde la fuente dicha" (Solomon, Barrett y Broom 2005).

b) ALGORITMOS AES

El estándar de cifrado (encriptación) avanzado AES, Advanced Encryption Standard (AES), es uno de los algoritmos más seguros y más utilizados hoy en día disponible para uso público. Está clasificado por la Agencia de Seguridad Nacional, National Security Agency (NSA), de los Estados Unidos para la seguridad más alta de información secreta "Top Secret".

Su historia de éxito comenzó 1997, cuando el Instituto Nacional de Estándares y Tecnología, National Institute of Standards and Technology (NIST), anunció la búsqueda de

un sucesor para el estándar de cifrado DES. Un algoritmo llamado “Rijndael”, desarrollado por los criptólogos belgas Joan Daemen y Vincent Rijmen, fue destacado en seguridad, así como en el rendimiento y la flexibilidad. Este algoritmo le gano a varios competidores, y fue oficialmente presentado como el nuevo estándar de cifrado AES en el 2001 y se transformó en estándar efectivo en el 2002.

El algoritmo se basa en varias sustituciones, permutaciones y transformaciones lineales, ejecutadas en bloques de datos de 16 bytes por lo que se le llama blockcipher. Estas operaciones se repiten varias veces, llamadas “rondas”. En cada ronda, un único “roundkey” se calcula de la clave de encriptación, y es incorporado en los cálculos.

Basado en esta estructura de bloque de AES, el cambio de un solo bit, ya sea en la clave, o en los bloques de texto simple y claro, resulta en un bloque de texto cifrado/encriptado completamente diferente – una clara ventaja sobre cifrados de flujo tradicionales.

La diferencia entre AES-128, AES-192 y AES-256, es la longitud de la clave: 128, 192 o 256 bits todos drásticamente mejorados en comparación con la clave DES de 56 bits. A modo de ejemplo: Descifrar una clave de 128 bits AES con una supercomputadora estándar del momento, llevaría más tiempo que la presunta edad del universo. ¡Boxcryptor utiliza incluso claves de 256! Hasta el día de hoy, no existe posible ataque contra AES. Por lo tanto, sigue siendo el estándar AES de cifrado preferido por los gobiernos, los bancos y los sistemas de alta seguridad de todo el mundo. (Herazo, 2015).

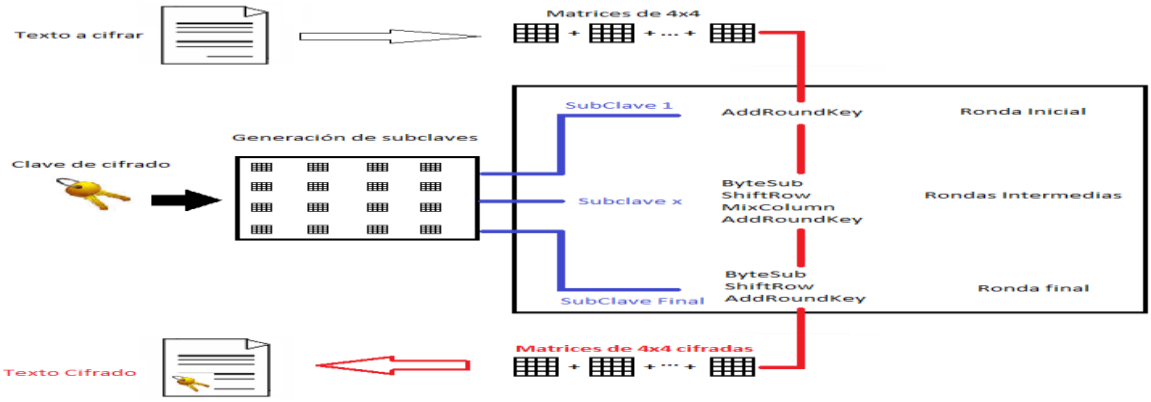


Figura 2. 3: Algoritmo AES
Fuente: José Mejías, 2014

2.6 SOFTWARE

"Para poder comprender los que es un software (y consecuentemente la ingeniería del software), es importante examinar las características del software que la diferencian de otras cosas que los hombres pueden construir. Cuando se construye hardware, el proceso creativo humano (análisis, diseño, construcción, prueba) se traduce finalmente en una forma física. Si construimos una nueva computadora, nuestro boceto inicial, diagramas formales de diseño y prototipo de prueba, evolucionan hacia un producto físico (chips, tarjetas de circuitos, impresos, fuentes de potencia, etcétera). El software es un elemento del sistema que es lógico, en lugar de físico. Por tanto el software tiene unas características considerablemente distintas a las del hardware. El software se desarrolla, no se fabrica en un sentido clásico" (Pressman, 2002).

2.7 KEYLOGGER

"Por sí mismo, el término 'keylogger' es neutral y describe una función que registra las pulsaciones de las teclas del ordenador. La mayoría de las fuentes consultadas definen keylogger como un programa diseñado para, en secreto, monitorear y registrar cada pulsación del teclado. Esta definición no es correcta del todo, pues un keylogger no necesariamente tiene que ser un programa, sino que también puede ser un dispositivo físico. Los dispositivos keylogger son menos conocidos que el software keylogger, que es importante tener en cuenta la existencia de ambos cuando se habla de seguridad informática" (Grebennikov, 2007).

2.8 MALWARE

"Al software malicioso, o malware, término que surge de las palabras en inglés 'malicious software', se le considera todo tipo de software cuyo objetivo es provocar daños a un sistema informático. Dentro del software malicioso o malware, el ejemplo más conocido es el del virus, es decir, un programa que actúa sobre otros programas, como una aplicación, el arranque, el registro del sistema,… Incluyéndose dentro de ellos y modificando su comportamiento. A este proceso se le conoce como infección, en comparación con el proceso que sufrimos los seres vivos cuando un virus nos ataca y afecta a nuestro organismo. Pero además el concepto de malware, es más extenso, ya que se puede considerar este tipo de

software no solo un virus, sino también los gusanos, troyanos y otros tipos" (García, Aguinaga y Mora, 2000).

2.9 USUARIO

"La mayor parte de los ordenadores que existe en la actualidad están diseñados de forma que puedan ejecutar diversas tareas o programas. Estos programas pueden ir desde un procesador de textos, a un programa para la animación de gráficos tridimensionales o distintos tipos de juegos. Para su correcto funcionamiento deben ser además capaces de acceder a los recursos de que dispone el ordenador, como por ejemplo escribir o leer datos de un disco duro, mostrar un gráfico por pantalla, etcétera. Es evidente, que si cada programa actuase de una forma independiente, existirían graves problemas y conflictos, puesto que, por ejemplo, tendría libertad para escribir sus datos sobre los de otro, etcétera. Los sistemas operativos son multitarea y multiusuario. Esto quiere decir que es capaz de ejecutar varios programas (o tareas) de forma simultánea y albergar varios usuarios de forma simultánea. Por los tanto un usuario es aquel que hace uso de una computadora" (García, Aguinaga y Mora, 2000).

2.10 PRIVACIDAD

"El concepto de privacidad, que inicialmente podía confundirse con la intimidad, adquiere una dimensión mucho más amplia con la incorporación de la informática como técnica imprescindible en todos los ámbitos sociales y económicos de la vida moderna. El hombre, para ser libre, debe defender del conocimiento de los demás, no sólo algunos aspectos íntimos de su vida privada que le hubieran podido definir como persona, sino que el campo de protección debe ser mucho más amplio: debe ser su privacidad" (Carreras, 2008).

2.11 TELÉFONO CELULAR

"Analizando la incidencia desde el punto de vista funcional, no hay dudas que el teléfono celular ha contribuido a mejorar las comunicaciones interpersonales. Es curioso pero a los jóvenes de hoy en día, les resulta increíble que en el pasado la gente no tuviera la posibilidad de comunicarse cuando estaba fuera de su hogar, o peor aún, debiera esperar una semana para hacer llegar un mensaje de texto, que en aquel entonces era una carta que dejaba

en manos del correo postal. Otro de los avances que traerá la tecnología del futuro serán las nuevas generaciones de chips de alta densidad. No es poca cosa si consideramos que gracias a ellos los celulares tendrán una capacidad de memoria enorme, lo que implica almacenar miles de fotos, videos, mails, grabaciones de voz y música" (Poratti, 2010).

2.12 SMARTPHONE

"El concepto de smartphone, implica o explícitamente consensuado, podría quedar reflejado en esta síntesis, suma de las diversas aportaciones de nuestros entrevistados: 'Un facilitador de comunicaciones sin fronteras, información de cualquier naturaleza facilitada y rápida, aparato que permite estar en contacto y enterarte de cosas. Su gran virtualidad está en la espontaneidad y la rapidez instantánea. Un aparato que parece estar ideado y hecho a la medida de la gente joven de nuestros días, aunque hay muchos adultos que se están integrando cada vez más en su uso y en todo lo que significa el universo smartphone" (Reig, 2013).

2.13 CRIPTOGRAFÍA

"La criptografía es un mecanismo que permite establecer canales de comunicaciones seguras entre dos puntos, cumpliendo además las características mencionadas en el punto anterior.

Cuando establecemos comunicación con otro equipo asumimos que nuestros mensajes son depositados generalmente en un medio hostil y necesitamos proveer sobre ellos cierta seguridad que permita su protección en los casos más desfavorables" (Blanco, 2014).

2.13.1 CRIPTOGRAFÍA SIMÉTRICA

La criptografía simétrica consiste en la utilización de una clave para cifrar un texto sin la cual no puede ser descifrado, por tanto, las dos partes de la comunicación necesitan saber la clave que cifra el mensaje.

Un esquema de cifrado simétrico tiene componentes:

- Mensaje plano: Es el mensaje legible que se mete al algoritmo como entrada.
- Algoritmo de cifrado: realiza varias transformaciones del mensaje plano.
- Clave de cifrado: Clave utilizada para cifrado.

- Texto cifrado: Este es el mensaje mezclado que se obtiene a la salida. Depende del mensaje plano y la clave.
- Algoritmo de descifrado: Acepta el texto cifrado y la correspondiente clave y produce el mensaje plano y la clave.

2.13.2 CRIPTOGRAFÍA ASIMÉTRICA

La criptografía asimétrica usa dos claves diferentes: una para el cifrado y otra para el descifrado. Las claves tienen una relación matemática especial que permite a los mansajes encriptados con una clave ser descifrados por la otra.

Normalmente en una aplicación criptográfica asimétrica, cada una de las partes de la comunicación tiene un par de claves. Una es conocida por las partes que participan en la comunicación y se llama clave pública. Esta clave puede ser guardada, administrada y difundida por determinados servidores. La otra clave que se utiliza, se llama clave privada y no puede ser conocida salvo por el dueño de dicha clave. Una de las partes de la comunicación puede cifrar el mensaje utilizando la clave pública, mientras que la otra parte de la comunicación descifrar este mensaje utilizando su clave privada.

Un esquema de cifrado de clave pública tiene componentes:

- Mensaje plano: Es el mensaje legible que se mete al algoritmo como entrada.
- Algoritmo de cifrado: Realiza varias transformaciones del texto llano.
- Clave pública y privada: Par de claves que han sido seleccionadas para que una se use para cifrado y otra para descifrado.
- Texto cifrado: Este es el mensaje mezclado que se obtiene a la salida. Depende del texto llano y la clave.
- Algoritmo de descifrado: Acepta el texto cifrado y la correspondiente clave y produce el texto llano original.

2.13.3 CRIPTOGRAFÍA HIBRIDA

Este sistema es la unión de las ventajas de los dos anteriores, debemos de partir que el problema de ambos sistemas criptográficos es que el simétrico es inseguro y el asimétrico lento. El proceso para usar un sistema criptográfico hibrido es el siguiente:

- Genera una clave pública y otra privada (en el receptor).
- Cifrar un archivo de forma síncrona.
- El receptor nos envía su clave pública.
- Ciframos la clave que hemos usado para encriptar el archivo con la clave pública del receptor.
- Enviamos el archivo cifrado (síncronamente) y la clave del archivo cifrada (asíncronamente y solo puede ver el receptor).

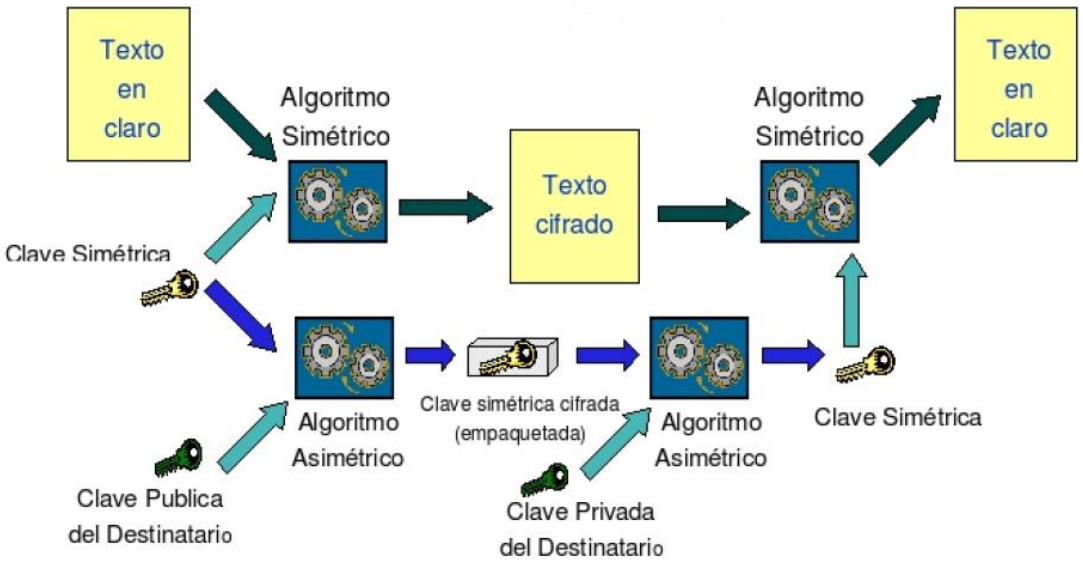


Figura 2. 4: Criptografía Híbrida
Fuente: criptografiaenbachilleraro.blogspot.com, 2017

2.14 RSA (Rivest, Shamir, Adleman)

Este algoritmo fue desarrollado en 1997 por Ron Rivest, Adi Shamir y Len Adleman en el MIT. El esquema RSA es un cifrado de bloques en el que el mensaje plano y el mensaje cifrado son enteros entre 0 y *n-1* dado un valor de *n*. Un tamaño típico para *n* es 1024 bits o 309 dígitos decimales.

Las claves obtenidas a partir de RSA sirven tanto para codificar como para autenticar. Es uno de los algoritmos asimétricos más seguros. Se basa en la dificultad para factorizar grandes números. Sin embargo, existen ciertos casos para los cuales el algoritmo RSA deja el mensaje original tal cual. Las claves pública y privada se calculan a partir de un número que se obtiene como producto de dos números primos grandes.

Actualmente se considera segura una clave RSA con una longitud de al menos 1024 bits, si bien se recomienda el uso de claves no inferiores a 2048 bits. (Blanco, 2014).

2.15 FTP (Protocolo de Transferencia de Archivos)

El FTP es uno de los sistemas de almacenamiento y distribución de archivos más populares de Internet. La sencillez con la que se realizan el montaje y el acceso, permiten a cualquier usuario acceder a archivos y carpetas remotas, casi como si se tratara de su propio disco duro.

FTP proviene de las siglas en inglés de File Transfer Protocol. Es un protocolo utilizado en forma específica para la transferencia de archivos a través de Internet. Así como usamos el HTTP para acceder a sitios web y el SMTP para el envío de correo electrónico, el FTP es parte de los protocolos del TCP/IP, que en este caso permiten trabajar con archivos y carpetas. Como se han de suponer, para poder trabajar con un FTP hace falta un servidor que aloje los archivos y al cual se le asigne una dirección FTP; la que nos servirá como “ruta” para acceder a los mismos. Si bien el propio Internet Explorer permite ingresar a la mayoría de los FTP para consultar o descargar su contenido, existen programas “cliente” que están desarrollados en forma específica para esa actividad. Mediante éstos, podemos subir o bajar información, modificarla, crear y borrar carpetas o archivos y todo cuanto hagamos con cualquier unidad local de nuestra PC. Gran parte de los servidores web utilizan el protocolo FTP, para que el diseñador pueda subir los archivos correspondientes al sitio que desea publicar allí. Esta práctica facilita en gran medida la tarea, ya que podemos transferir archivos en grandes cantidades, como si los copiáramos de una unidad a otra de la PC. (Quinodóz, 2017).

CAPITULO III

MARCO APLICATIVO

Supongamos que desempeña un trabajo en una organización, en la cual existe competencia con otras organizaciones del mismo rubro. La organización como tal debe estar equipada en la actualidad con tecnología y recursos humanos competentes. La mayor parte de los empleados van a tener acceso a un dispositivo móvil entregado como instrumento de trabajo un bien de la organización, por ejemplo algunos usuarios podrán crear documentos planillas de registros de productos entre otros. Son éstos usuarios y sus dispositivos móviles considerados puntos críticos ya que la información que pasa a través de estos está íntimamente relacionada a la organización.

Un usuario, tomemos el caso de un empleado encargado de repartir productos, registrar productos pedidos por el cliente en cualquier mercado formal o informal, puede o no estar desarrollando sus actividades cotidianas con el dispositivo móvil, no obstante llegará un momento en el cual el usuario estará chateando, jugando juegos en línea o fuera de línea, escuchando música, viendo videos, etc., desarrollando actividades personales y no así las relacionadas a la organización, de suponer que en otro momento el usuario posee información relevante como ser estados financieros de los clientes a la hora de pedir productos, contacto de clientes o supervisores, etc., estos usuarios pueden ser fácilmente sobornables por otras personas interesadas en esa información para ser vendida a las organizaciones en competencia,

por ejemplo puede darse el caso de que este usuario copie esta información y lo mande por correo electrónico o por alguna aplicación que se encuentre en el dispositivo móvil.

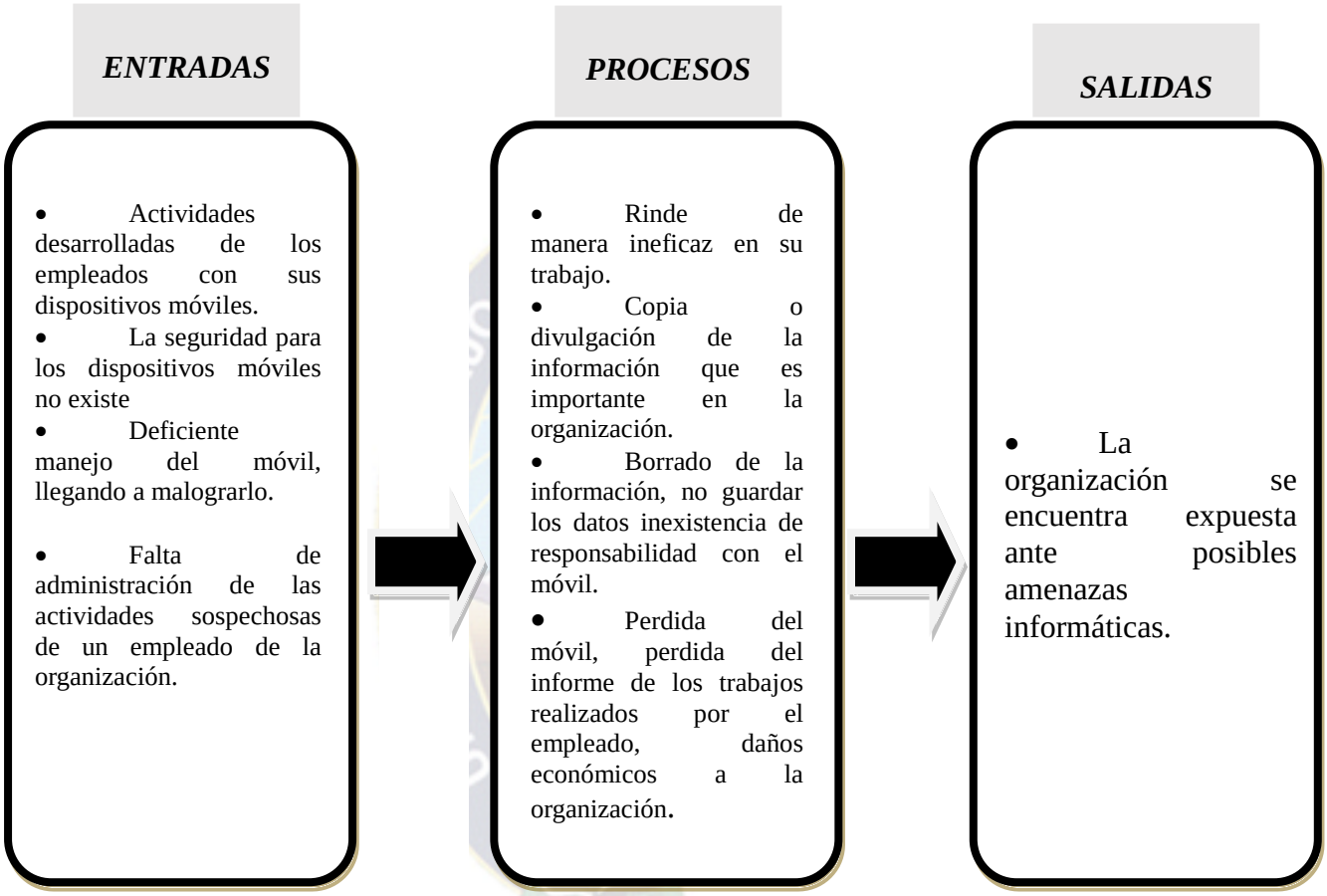


Figura 3. 1: Modelo Entrada Proceso Salida en la Organización

Ahora bien se debe hacer un análisis de esta situación o de alguna otra situación parecida, en el presente la información sobre una organización es muy importante y el acceso no es igual para los usuarios de acuerdo al organigrama y políticas que tienen las organizaciones.

Cuando el usuario realiza sus actividades con su dispositivo móvil en condiciones normales, puede que este con el cliente o este solo, lo cual implica que éste puede estar trabajando o como también no puede estar trabajando, en definitiva nadie lo sabe, solo el mismo usuario responde a sus acciones. Es de aquí que surge también la distracción dentro

del trabajo encomendado. Puede que necesite realizar un informe de los pedidos de productos por ejemplo, otro punto negativo que nace es el manipular el dispositivo móvil sin ninguna responsabilidad olvidando guardar los pedidos de los clientes dando mayor importancia a los mensajes de Whatsapp, Facebook de sus amigos, el caso también que el usuario baje por internet aplicaciones que tengan virus y que contagien el dispositivo como por ejemplo abrir ventanas a enlaces externos y realice descargas no autorizadas o envié datos importantes del dispositivo.

Un típico caso es que la organización pone una demanda al empleado por obtener y copiar información de la organización hacia terceras personas, el empleado por su parte se defiende y dice que el dispositivo móvil se extravió o que cualquier otro empleado pudo haber hecho esta acción y no así él.

Se pueden observar que pueden ser muchos los casos que se pueden dar para que el activo más importante de la organización se vea comprometido como la información, he aquí surgen varias preguntas y dudas sobre el ¿Cómo saber?, ¿Qué hacer?, es que ¿se debe confiar en la ética de los empleados?, es que ¿se debe contratar otros empleados?, etc...

Entonces se puede deducir que las amenazas informáticas a las que la organización está expuesta, provienen en su gran mayoría internamente por parte de las acciones de los empleados, debido a diferentes motivaciones.

3.1 APLICACIÓN DE LA METODOLOGIA DE VERISIGN IDEFENSE

VeriSign iDefense Security Intelligence Service (Servicio de inteligencia de seguridad de VeriSign iDefense), posee una metodología para la seguridad de los certificados SSL (Secure Sockets Layer o Capa de Sockets Seguro) que normalmente son utilizados en sitios web seguros, como el caso de los bancos o tiendas electrónicas donde se hace uso de las tarjetas de crédito. La metodología con la que se trabaja sigue cuatro etapas para el control de la información: *Descubrimiento, Análisis, Publicación y Entrega.*

La herramienta que se está proponiendo, análogamente va a seguir esta metodología de trabajo. En una primera etapa de "*descubrimiento*" la herramienta utiliza un "monitoreo" constante del empleado cuando éste haga uso de su dispositivo móvil, el cómo lograrlo, Se

realizara una captura de todo lo tecleado en la pantalla por el usuario, las aplicaciones que esté ejecutando a lo largo del día, realizando capturas de pantalla cada cierto tiempo. Por otra parte, se debe proteger la privacidad del usuario de acuerdo a las políticas internas de la organización.

En cuanto a la etapa de "*análisis*" de la información recolectada, el software propuesto presenta un módulo de reportes (como cualquier otro sistema informático), el cual está encargado en mostrar la recolección de información manipulada por el usuario, dicho de otro modo mostrara las capturas de texto, mostrara las aplicaciones ejecutadas durante todo el día, mostrara las capturas de pantalla, se realizara un análisis de las posibles amenazas que surjan y búsquedas dentro de la información recolectada.

En cuanto a la "*publicación*", los reportes van a permitir que el análisis sea más eficiente, pues al momento de visualizar las capturas ya sea de texto o de imágenes, darán a conocer las vulnerabilidades que puedan existir del usuario, No se debe olvidar que lo que se ha capturado mediante el monitoreo debe ser encriptado, para que sea ilegible ante los ojos del usuario.

En la parte de "*entrega*", se lo realiza cuando los encargados del monitoreo de la organización piden al empleado entregar el dispositivo móvil para una actualización de su sistema operativo y mantenimiento de alguna otra aplicación de la organización, lo cual permitirá al usuario de la aplicación ver los reportes y capturas de pantalla registradas, también se lo realizara vía FTP (Protocolo de Transferencia de Archivos). Pero para esta entrega el software lo ha de tomar como backup (copia de seguridad), dado que el programa tiene objetivos precisos, puede ser considerado como malicioso o de naturaleza ambigua, lo cual implica que puede ser desactivada.

3.2 CONSTRUCCIÓN DEL SOFTWARE

Durante la fase de desarrollo, la aplicación es codificada y analizada. Las tareas a llevarse a cabo durante la fase de desarrollo van a incluir el determinar cualquier requerimiento restante, desarrollar el prototipo del software y probar el mismo.

3.2.1 DESCRIPCIÓN DEL PROTOTIPO

El software es desarrollado bajo los siguientes requerimientos mínimos:

Software: Sistema Operativo Android, Android Studio (IDE) versión 2.3, lenguaje Java.

Hardware: Dispositivo Móvil, 1.2 GHz dual-core, 512MB RAM, 100 MB de Disco Duro.

Android es un sistema operativo basado en el núcleo Linux. Fue diseñado principalmente para dispositivos móviles con pantalla táctil, como teléfonos inteligentes, tablets y también para relojes inteligentes, televisores y automóviles, está presente en la mayoría de los equipos corporativos de las organizaciones.

3.2.2 ORGANIZACIÓN DEL SOFTWARE

Cuando se desarrolla un software, se debe tener en claro la manera en que se organiza el código, como está estructurado. El software está desarrollado de manera estructurado, lo que implica la existencia de módulos. La figura 3.2.1 muestra la modularización del software.

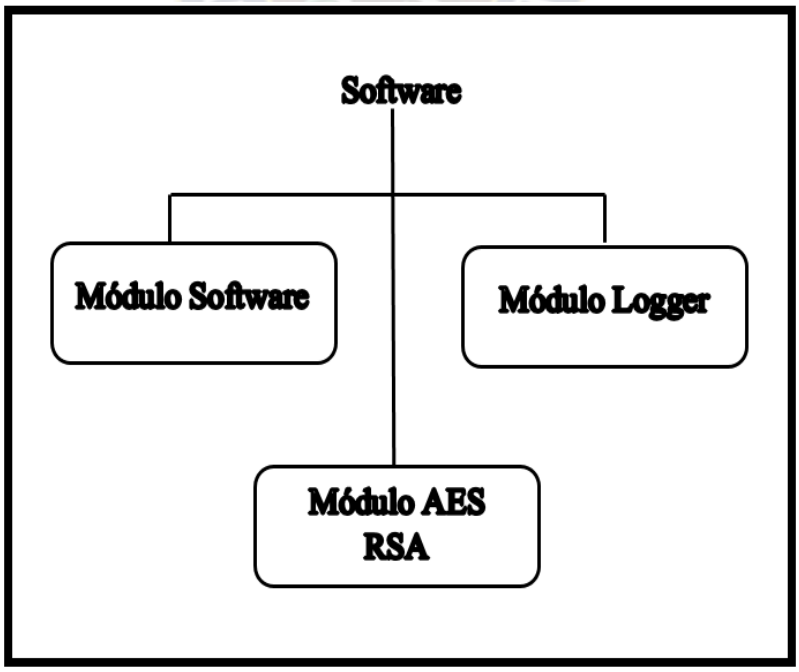


Figura 3. 2: Modularización del Software

Módulo Software: está encargado de realizar las configuraciones, en este módulo se encuentra los reportes.

Módulo AES RSA: está encargado de realizar el proceso de encriptación, proveyendo métodos para ser utilizados en los demás módulos.

Módulo Logger: está encargado de realizar el monitoreo de las actividades realizadas por parte del empleado cuando éste haga uso del dispositivo móvil.

3.2.3 ESTRUCTURA DEL CÓDIGO

Dentro del Módulo Software, se encuentran los siguientes archivos:

- Interfaz gráfica del usuario, donde se encuentra las configuraciones y selección de los reportes requeridos.
- Autentificación del usuario, que en este caso será el administrador, ya que es éste el que obtendrá los reportes.
- Código necesario para presentar reportes, análisis de archivos, búsquedas, etc.
- Lista de palabras clave, que ayuda a identificar cuándo el usuario necesite privacidad y confidencialidad.

Dentro del Módulo AES RSA, se encuentran los siguientes archivos:

- Rutinas para simular el algoritmo Rijndael, denominado Advanced Encryption Standard, su codificación es simple pero el algoritmo es uno de los estándares que ofrece una seguridad impresionante.
- Codificación y decodificación de bytes, haciendo uso de las librerías criptográficas.
- Implementación de los anteriores códigos, provee dos métodos: uno para encriptar y otro para des encriptar.

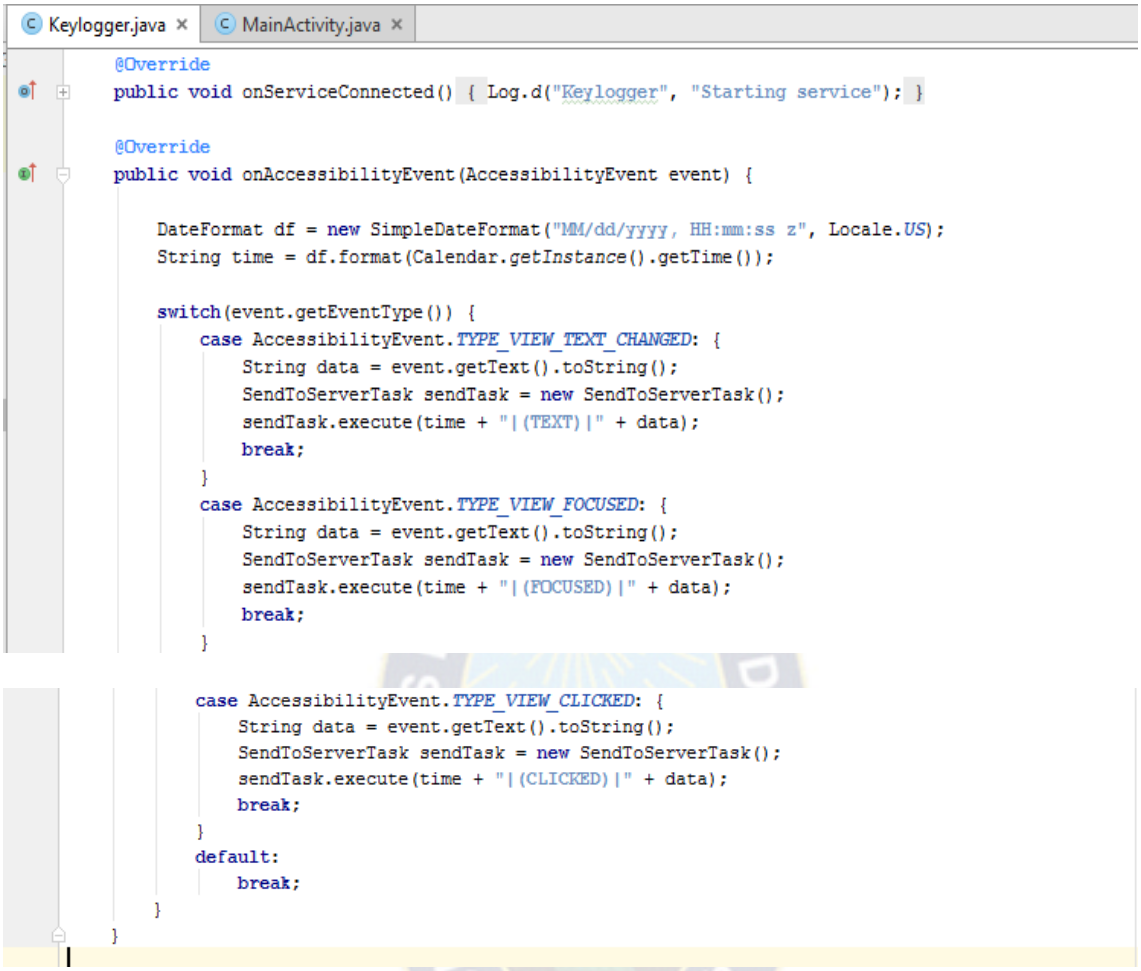
Dentro del Módulo Logger, se encuentra los siguientes archivos:

- Variables globales configurables de la herramienta.
- Procedimientos y funciones que van a permitir el monitoreo de las acciones realizadas en un dispositivo móvil.
- Encargado de que este Módulo sea residente en memoria durante la ejecución del Sistema.

3.2.4 DESCRIPCIÓN DEL PROCESO DE MONITOREO

Al referirse a la palabra monitoreo, hablamos del hecho de estar al tanto de lo que sucede en un momento y lugar determinado, se está refiriendo a custodiar, mantener, guardar, observar. Para poner esto en la práctica, se va a implementar un keylogger, el cual es un programa informático que registra las pulsaciones que se realizan sobre el teclado de la pantalla del dispositivo móvil para ser guardadas en un archivo o ser enviadas por internet. Se encuentran disponibles un gran número de programas que permiten a los administradores rastrear las actividades diarias de los empleados en sus ordenadores, actualmente en los países desarrollados implementan este software para monitorear a sus empleados mediante los dispositivos móviles que son activos de las empresas los cuales cuentan con información de las mismas. Sin embargo, el límite ético entre el monitoreo justificado y el espionaje delincuencial suele ser muy tenue. Sucede que a menudo los programas legítimos son utilizados de manera deliberada para robar información confidencial del usuario, como por ejemplo sus contraseñas.

A continuación se muestra el código que utiliza el keylogger para capturar las pulsaciones del dispositivo móvil, ubicado en el directorio src\java\keylogger:



```
Keylogger.java × | MainActivity.java ×

    @Override
    public void onServiceConnected() { Log.d("Keylogger", "Starting service"); }

    @Override
    public void onAccessibilityEvent(AccessibilityEvent event) {

        DateFormat df = new SimpleDateFormat("MM/dd/yyyy, HH:mm:ss z", Locale.US);
        String time = df.format(Calendar.getInstance().getTime());

        switch(event.getEventType()) {
            case AccessibilityEvent.TYPE_VIEW_TEXT_CHANGED: {
                String data = event.getText().toString();
                SendToServerTask sendTask = new SendToServerTask();
                sendTask.execute(time + "|(TEXT)|" + data);
                break;
            }
            case AccessibilityEvent.TYPE_VIEW_FOCUSED: {
                String data = event.getText().toString();
                SendToServerTask sendTask = new SendToServerTask();
                sendTask.execute(time + "|(FOCUSED)|" + data);
                break;
            }

            case AccessibilityEvent.TYPE_VIEW_CLICKED: {
                String data = event.getText().toString();
                SendToServerTask sendTask = new SendToServerTask();
                sendTask.execute(time + "|(CLICKED)|" + data);
                break;
            }
            default:
                break;
        }
    }
```

Programa 3. 1: Método onAccessibilityEvent

En la figura anterior se puede observar que el método onAccessibilityEvent que representa la clase AccessibilityEvent, evento de accesibilidad que son enviados por el sistema cuando algo notable ocurre en la interfaz de usuario. También se está definiendo SimpleDateFormates una clase concreta para dar formato y analizar fechas en una forma local. Calendar.getInstance().getTime( ), proporciona un método de clase getInstance, para obtener un objeto generalmente útil de este tipo. Calendar getInstance devuelve un Calendario objeto cuyos campos de calendario han sido inicializados con la fecha y hora actuales, getTime() devuelve el número en milisegundos. A continuación observamos la instrucción Switch el cual es una forma de anidamiento múltiple de instrucciones if… else, para tener una mayor claridad del código, TYPE_VIEW_TEXT_CHANGED representa evento de cambiar el texto de un archivo, TYPE_VIEW_FOCUSED representa el evento de enfoque,

TYPE_VIEW_CLICKED representa el evento de clic en la interfaz de usuario.

Por otro lado en el directorio src\java\MainActivity se tiene el código:

Keylogger.java × MainActivity.java ×

```
import android.os.AsyncTask;
import android.os.Looper;
import android.support.v7.app.AppCompatActivity;
import android.os.Bundle;
import android.util.Log;

import java.io.DataOutputStream;

public class MainActivity extends AppCompatActivity {

    private class Startup extends AsyncTask<Void, Void, Void> {
        @Override
        protected Void doInBackground(Void... params) {

            enableAccessibility();
            return null;
        }
    }

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        Log.d("MainActivity", "onCreate");

        setContentView(R.layout.activity_main);

        (new Startup()).execute();
    }
```

```
    void enableAccessibility(){
        Log.d("MainActivity", "enableAccessibility");
        if (Looper.myLooper() == Looper.getMainLooper()) {
            Log.d("MainActivity", "on main thread");

        } else {
            Log.d("MainActivity", "not on main thread");

            try {
                Process process = Runtime.getRuntime().exec("su");
                DataOutputStream os = new DataOutputStream(process.getOutputStream());
                os.writeBytes("settings put secure enabled_accessibility_services com.Prototipo.....
                os.flush();
                os.writeBytes("settings put secure accessibility_enabled 1\n");
                os.flush();
                os.writeBytes("exit\n");
                os.flush();

                process.waitFor();
            } catch (Exception e) {
                e.printStackTrace();
            }
        }
    }

}
```

Programa 3. 2: Clase AsyncTask

En la figura anterior se puede observar que la clase AsyncTask permite un uso adecuado y sencillo del subproceso de interfaz de usuario. Esta clase le permite realizar operaciones en segundo plano y publicar resultados en el subproceso de interfaz de usuario sin tener que manipular subprocesos y / o controladores.

3.2.5 DESCRIPCIÓN DEL PROCESO DE ENCRIPTACIÓN

Una combinación muy habitual en la criptografía híbrida consiste en el cifrado simétrico de los datos útiles mediante AES y el consiguiente descifrado asimétrico de la clave de sesión con RSA. A continuación se observara los distintos las clases y métodos que se empleó en el desarrollo del software:

```
import android.app.Activity;
import android.os.AsyncTask;
import android.os.Bundle;
import android.support.annotation.Nullable;
import android.text.TextUtils;
import android.util.Log;
import android.view.Menu;
import android.view.MenuItem;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;

import org.ow2.util.base64.Base64;

import java.io.ByteArrayInputStream;
import java.io.ByteArrayOutputStream;
import java.io.UnsupportedEncodingException;
import java.security.KeyPair;
import java.util.Arrays;

public class EncryptionActivity extends Activity {


    private EditText decryptedText = null, encryptedText = null, inputtedUnencryptedText = null ;


    private KeyPair rsaKey = null;


    private byte[] encryptedAESKey = null;
```

Programa 3. 3: Clase EncryptionActivity

En la figura anterior se puede observar que la clase EncryptionActivity se da un par de claves (público y privado) en RSA, en el cifrado AES va combinado la clave.

AESEncryptDecrypt.java × | EncryptionActivity.java × | Base64.java × | RSAEncryptDecrypt.java × | Cipher.java ×

```
import android.util.Log;
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.io.UnsupportedEncodingException;
import java.security.AlgorithmParameters;
import java.security.NoSuchAlgorithmException;
import java.security.NoSuchProviderException;
import java.security.Provider;
import java.security.Security;
import java.security.spec.InvalidKeySpecException;
import java.security.spec.KeySpec;
import javax.crypto.Cipher;
import javax.crypto.CipherInputStream;
import javax.crypto.CipherOutputStream;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.PBEKeySpec;
import javax.crypto.spec.SecretKeySpec;

    public class AESEncryptDecrypt {

        public static final String NOT_SECRET_ENCRYPTION_KEY = "12345678123456781234567812345678";
        public static final String SECRET_KEY_TYPE = "MNBVC7ContPmacSHA7";
        public static final String salt = "some_salt";
        public static final int KEY_LENGTH = 256;
        public static final int ITERATION_COUNT = 65536;
        public static final String AES = "AES";
        public static String SECURITY_PROVIDER = "SC";
```

Programa 3. 4: Clase AESEncryptDecrypt

En la figura anterior se puede observar que la clase AESEncryptDecrypt se observa una clave de 32 byte con un tipo de clave de AES que se creará con un valor utilizado para el salto el cual puede ser cualquier otro, definiendo la longitud de la clave con una iteración de veces de la contraseña.

AESEncryptDecrypt.java | EncryptionActivity.java | Base64.java | RSAEncryptDecrypt.java | Cipher.java

```
import android.util.Log;
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.NoSuchAlgorithmException;
import java.security.PrivateKey;
import java.security.PublicKey;

import javax.crypto.Cipher;

public class RSAEncryptDecrypt {


    public static final int KEY_LENGTH = 2048;

    public static final String RSA = "RSA";
```

Programa 3. 5: Clase RSAEncryptDecrypt

En la figura anterior se puede observar que la clase RSAEncryptDecrypt definimos la longitud de la clave, en el cual se está generando una clave RSA de 2048 bits y devolverá una clave de 2048 bits.

AESEncryptDecrypt.java | EncryptionActivity.java | Base64.java | RSAEncryptDecrypt.java | Cipher.java

```
package org.ow2.util.base64;

public class Base64 {

    private static char[] alphabet =
        "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/="
        .toCharArray();

    private static byte[] codes = new byte[256];

    static {
        for (int i = 0; i < 256; i++) {
            codes[i] = -1;
        }
        for (int i = 'A'; i <= 'Z'; i++) {
            codes[i] = (byte) (i - 'A');
        }
        for (int i = 'a'; i <= 'z'; i++) {
            codes[i] = (byte) (26 + i - 'a');
        }
        for (int i = '0'; i <= '9'; i++) {
            codes[i] = (byte) (52 + i - '0');
        }
        codes['+'] = 62;
        codes['/'] = 63;
    }
```

```
public static char[] encode(byte[] data) {
    char[] out = new char[((data.length + 2) / 3) * 4];


    for (int i = 0, index = 0; i < data.length; i += 3, index += 4) {
        boolean quad = false;
        boolean trip = false;

        int val = (0xFF & (int) data[i]);
        val <<= 8;
        if ((i + 1) < data.length) {
            val |= (0xFF & (int) data[i + 1]);
            trip = true;
        }
        val <<= 8;
        if ((i + 2) < data.length) {
            val |= (0xFF & (int) data[i + 2]);
            quad = true;
        }
        out[index + 3] = alphabet[(quad ? (val & 0x3F) : 64)];
        val >>= 6;
        out[index + 2] = alphabet[(trip ? (val & 0x3F) : 64)];
        val >>= 6;
        out[index + 1] = alphabet[val & 0x3F];
        val >>= 6;
        out[index + 0] = alphabet[val & 0x3F];
    }
    return out;
}
```

```
public static byte[] decode(char[] data) {


    int tempLen = data.length;
    for (int ix = 0; ix < data.length; ix++) {
        if ((data[ix] > 255) || codes[ data[ix] ] < 0) {
            --tempLen;
        }
    }


    int len = (tempLen / 4) * 3;
    if ((tempLen % 4) == 3) {
        len += 2;
    }
    if ((tempLen % 4) == 2) {
        len += 1;
    }

    byte[] out = new byte[len];



    int shift = 0;
    int accum = 0;
    int index = 0;
```

```
        for (int ix = 0; ix < data.length; ix++) {
            int value = (data[ix] > 255) ? -1 : codes[ data[ix] ];

            if (value >= 0) {
                accum <<= 6;
                shift += 6;
                accum |= value;
                if (shift >= 8) {
                    shift -= 8;
                    out[index++] =
                        (byte) ((accum >> shift) & 0xff);
                }
            }

        }


        if (index != out.length) {
            throw new Error("Miscalculated data length (wrote " + index + " instead of " + out.length + ")");
        }

        return out;
    }


}
```

Programa 3. 6: Clase Base64.java

En la figura anterior se puede observar que la clase Base64.java, proporciona codificación de bytes sin formato a caracteres codificados en base64 y decodificación de caracteres base64 a bytes sin formato. Donde los caracteres de código darán valores de 0...63, con una tabla de búsqueda para convertir caracteres base64 a un valor en el rango 0...63, donde devuelve una matriz de caracteres codificados en base64 para representar la matriz de datos. En los parámetros se encontrara la matriz de dato en bytes para codificar, en la devolución la matriz de caracteres codificados en base64. En proceso se puede observar a 3 bytes que codifican a 4 caracteres. La salida es siempre múltiplo de 4 caracteres.

Decodificada una secuencia codificada base64 para recuperar los datos originales. El espacio en blanco antes y después se recortará, pero no se realizará ninguna otra manipulación de la entrada. Este método maneja correctamente la entrada que contenga caracteres no deseados, en los parámetros el dato de flujo es codificado a base64 y la devolución es de datos originales.

AESEncryptDecrypt.java × | EncryptionActivity.java × | Base64.java × | RSAEncryptDecrypt.java × | Cipher.java ×

```
package javax.crypto;

import ...


public class Cipher {

    private static final Debug debug =
                         Debug.getInstance("jca", "Cipher");

    public static final int ENCRYPT_MODE = 1;

    public static final int DECRYPT_MODE = 2;

    public static final int WRAP_MODE = 3;

    public static final int UNWRAP_MODE = 4;

    public static final int PUBLIC_KEY = 1;

    public static final int PRIVATE_KEY = 2;

    public static final int SECRET_KEY = 3;
```

```
    private Provider provider;

    private CipherSpi spi;

    final private String transformation;

    final private String[] tokenizedTransformation;

    private ExemptionMechanism exmech;

    private boolean initialized = false;


    private int opmode = 0;

    private static final String KEY_USAGE_EXTENSION_OID = "2.5.29.15";

    private final SpiAndProviderUpdater spiAndProviderUpdater;
```

```
protected Cipher(CipherSpi cipherSpi,
                 Provider provider,
                 String transformation) {
    if (cipherSpi == null) {
        throw new NullPointerException("cipherSpi == null");
    }
    if (!(cipherSpi instanceof NullCipherSpi) && provider == null) {
        throw new NullPointerException("provider == null");
    }

    this.spi = cipherSpi;
    this.provider = provider;
    this.transformation = transformation;
    this.tokenizedTransformation = null;

    this.spiAndProviderUpdater =
        new SpiAndProviderUpdater(provider, cipherSpi);
}

private Cipher(CipherSpi cipherSpi,
               Provider provider,
               String transformation,
               String[] tokenizedTransformation) {
    this.spi = cipherSpi;
    this.provider = provider;
    this.transformation = transformation;
    this.tokenizedTransformation = tokenizedTransformation;

    this.spiAndProviderUpdater =
        new SpiAndProviderUpdater(provider, cipherSpi);
}
```

Programa 3. 7: Clase Cipher.java

En la figura anterior se puede observar que la clase proporciona la funcionalidad de un cifrado criptográfico para cifrado y descifrado. Forma el núcleo del marco de JCE (Java Crytographic Extension). Para crear un objeto cipher, la aplicación llama al getInstance método cipher y le pasa el nombre de la transformación solicitada. Opcionalmente, se puede especificar el nombre de un proveedor.

Una transformación es una cadena que describe la operación (o conjunto de operaciones) que realizará en la entrada dada, para producir algo de salida. Una transformación siempre incluye el nombre de un algoritmo criptográfico y puede ser seguido por un modo de realimentación y un esquema de relleno como se observa.

3.3 INTERFAZ DE USUARIO.

La interfaz de usuario está compuesta por vista (view) layout, es un conjunto de vistas agrupadas de una determinada forma vamos a disponer de diferentes tipos de layouts para organizar las vistas, siendo agradable y sencilla a la vista del usuario. El prototipo consta de

siete layouts (vistas), se entiende por layout como una estructura visual para una interfaz de usuario, es decir, aquello que hace de intermediario entre el terminal móvil y el usuario. Un elemento de interfaz de usuario se puede declarar desde un fichero XML o en tiempo de ejecución de la aplicación.

Existe un conjunto de fases que se deben satisfacer para establecer una comunicación exitosa y se cumpla el objetivo perseguido. En el primer layout de inicio se observa un logo de bienvenida a la aplicación de color rojo por representar un fuerte grado de dignidad y orgullo como se puede ver en la Figura 3.3.

Figura 3. 3: Pantalla de presentación

En el segundo layout, para que el usuario pueda registrarse en la aplicación y obtener los privilegios asociados a su cuenta, donde se debe introducir nombre del usuario y su contraseña, en el caso de ser la primera vez se debe ingresar a la opción ¿No tiene cuenta? Como se puede ver en la Figura 3.4.

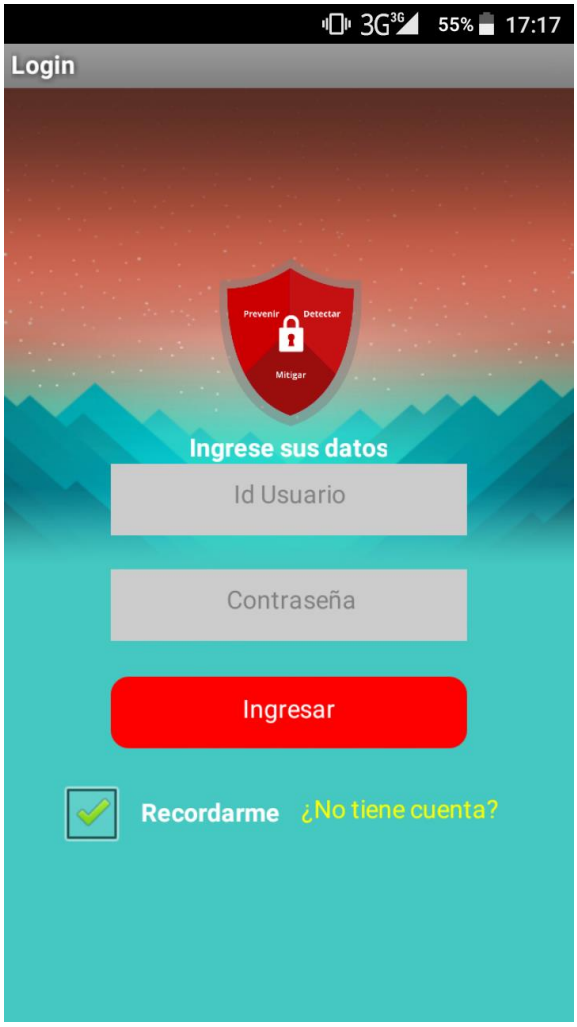


Figura 3. 4: Usuario y contraseña

El tercer layout encontramos un logo y un menú con seis opciones las cuales nos llevan a cada una de ellas para las acciones a ser utilizadas que se describirán más adelante, a continuación se observa la Figura 3.5.

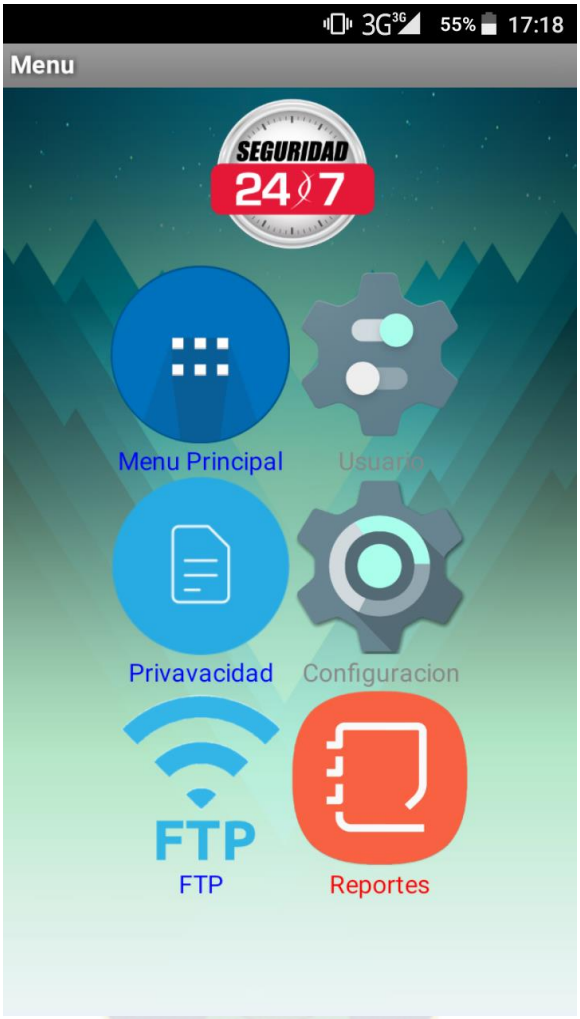


Figura 3. 5: Menú

Al ingresar al primer icono con nombre Menú Principal se observa las instrucciones de cada icono donde se debe de configurar antes de su inicialización, lo primero es crear una cuenta de usuario, Figura 3.6.

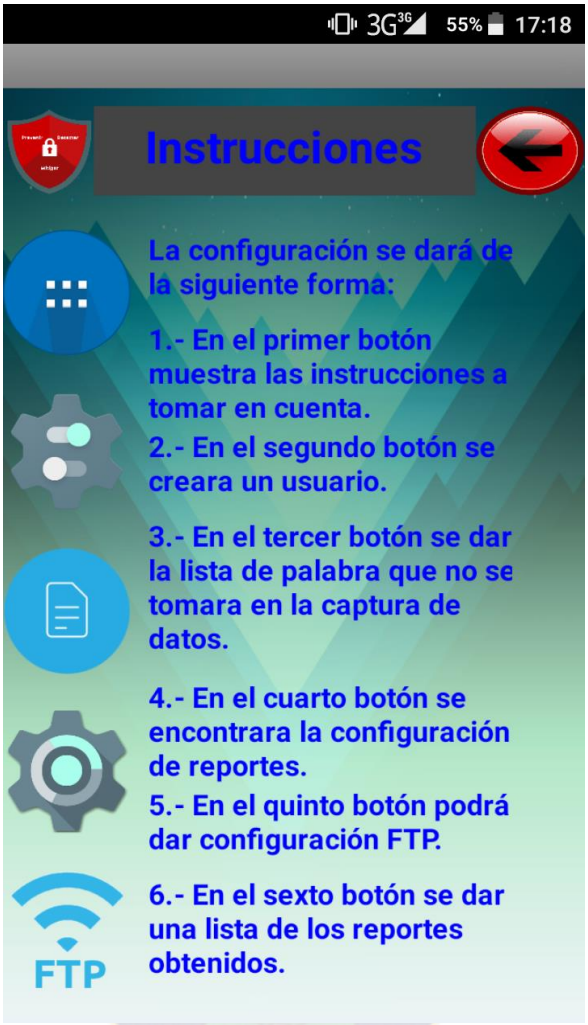


Figura 3. 6: Instrucciones

En el cuarto layout se observa la configuración de cuenta de usuario, para la primera vez se tendrá que crear un usuario para que pueda iniciar la aplicación correctamente con su usuario y contraseña sin olvidar la habilitación del mismo Figura 3.7.

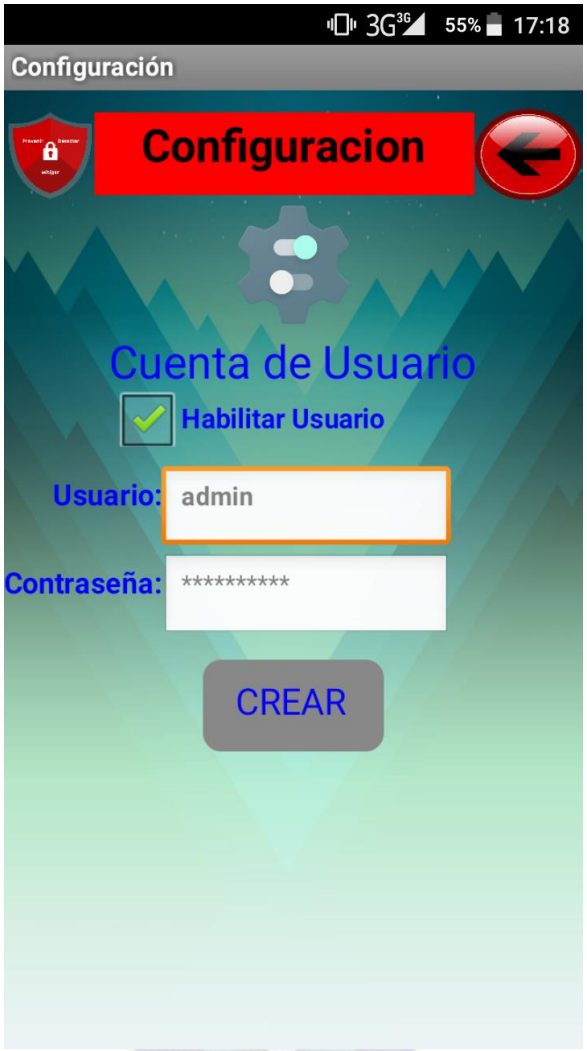


Figura 3. 7: Configuración

En el icono de Confidencialidad podremos escribir las palabras que la aplicación no tomara en cuenta respetando su privacidad del usuario, el cual tendrá dos botones el de insertar la palabra y el de guardar respectivamente, Figura 3.8.

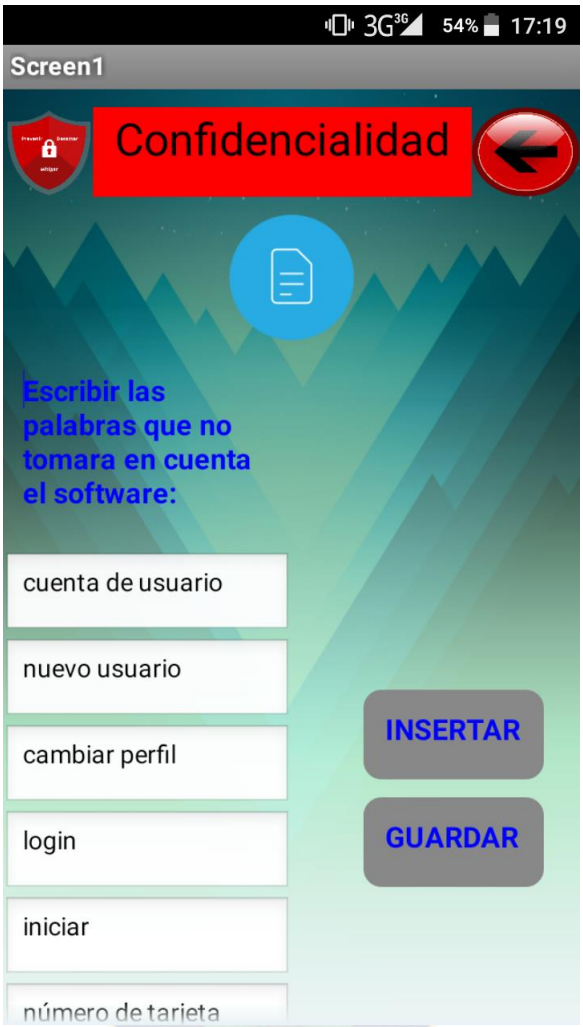


Figura 3. 8: Confidencialidad

Se toma en cuenta de la implementación de un DatePicker (Selector de fechas) para una mejor busca de fechas, cuando el usuario haga clic sobre un EditText de solo lectura (donde necesitamos la fecha), presionando el botón mostrar se abrirá el reporte de la fecha buscada, también la opción de buscar texto y ser mostrado, analizar el archivo y ver las capturas de pantallas. Figura 3.9.

Figura 3. 9: Reportes

En la siguiente vista tenemos la opción de configurar la copia de seguridad de los archivos que contiene las capturas, resultado del proceso de monitoreo y que serán enviados por FTP, en el cual se requiere ingresas los siguientes datos como ser: servidor, puerto, usuario, contraseña, backup con un tiempo en minutos y con los respectivos botones de aplicar y borrar el contenido. Figura 3.10.

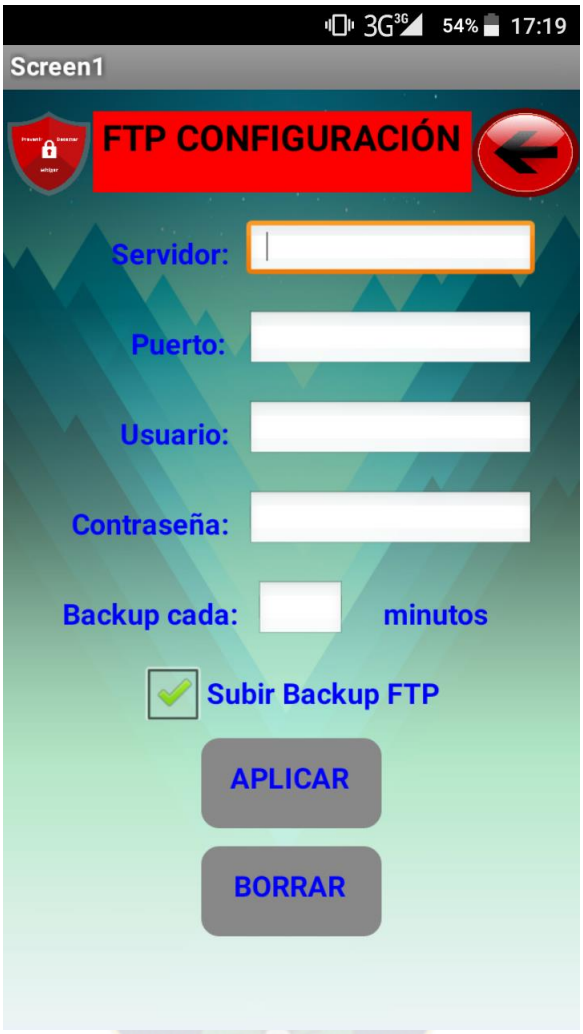


Figura 3. 10: FTP Configuración

3.4 PRUEBAS DEL PROTOTIPO.

Después de la construcción del prototipo, es necesario ahora pasar al análisis de resultados. Para la evaluación se requiere realizar distintas pruebas dándonos casos donde existan empleados distintos cada uno para la evaluación del prototipo si realmente cumple los objetivos.

Primera prueba, supongamos que un empleado con este dispositivo móvil que es un activo de alguna organización que esté trabajando. Se desea saber si en realidad hizo su trabajo. A continuación en la Figura 3.11 observamos que se seleccionó el icono de reportes y se realizó un análisis del archivo de fecha 30.11.2017, como nos muestra la Figura 3.11.

Figura 3. 11: Primera prueba

En conclusión se puede observar que el empleado no ha ejecutado ninguna aplicación que afecte su trabajo diario, simple mente hizo uso de las aplicaciones, entonces se puede concluir que el empleado no representa alguna amenaza informática para la organización.

Segunda prueba, si un empleado es notado en la organización como una posible amenaza informática y existen pruebas estas podrían ayudar de gran manera a la organización por ejemplo en el dispositivo móvil del empleado se pudo observar que en la captura de pantallas que realizo el prototipo el trabajador estaba realizando actividades distintas a las encomendadas, visitando páginas de juegos, chats, Facebook, ingresando a configuración del dispositivo móvil para borrar aplicaciones, copiar planillas de clientes de una determinada fecha que solo tiene importancia a la organización.

Por lo tanto se puede concluir del empleado es realmente una amenaza informática para la organización, además que en esta prueba el prototipo ha sido efectivo al momento de brindar los reportes. Figura 3.12.

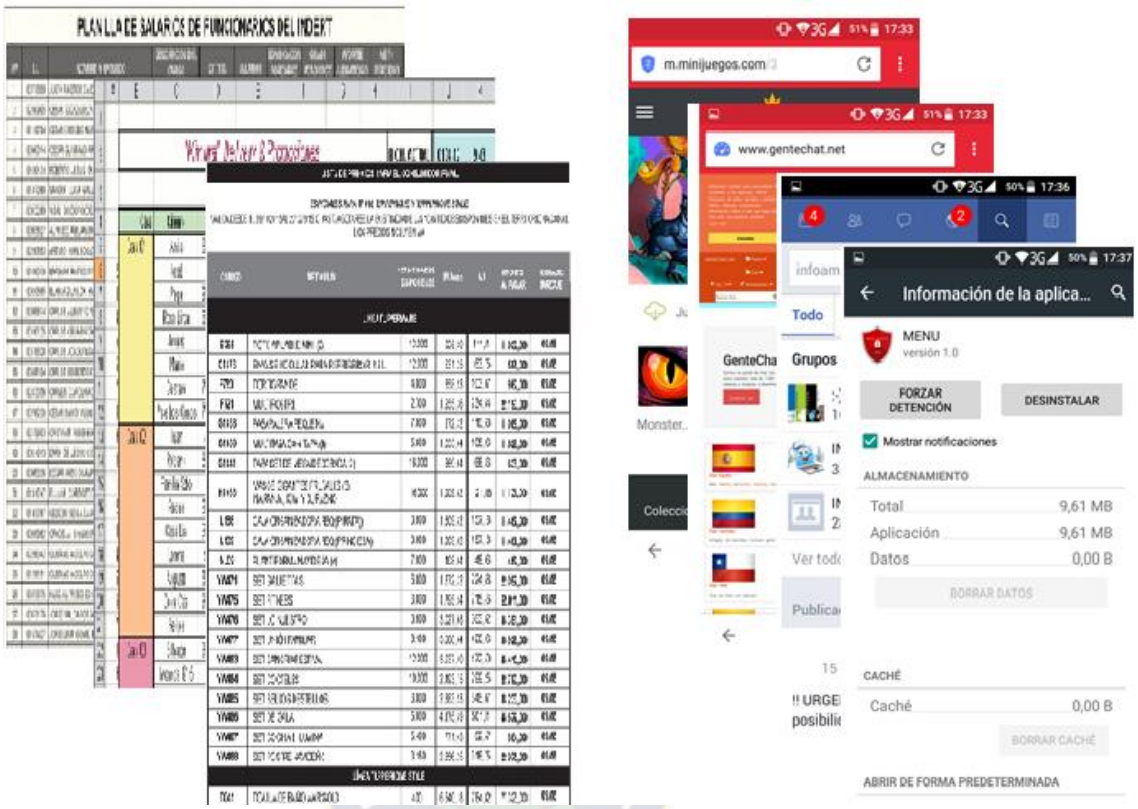


Figura 3. 12: Captura de pantallas

Tercera prueba, el empleado en momentos de descanso se pone a investigar dentro del dispositivo móvil viendo las carpetas, si hay algo raro abriendo los archivos que existen y borrarlos si lo involucran a él por ejemplo, por algún otro compañero de trabajo que le haya comentado que él está siendo vigilado, si el empleado llego a encontrar la aplicación y quiere desinstalarla el no podrá, porque se instaló como un servicio del sistema Android lo cual será complicado la desinstalación del mismo, también si observa la existencia de archivos de texto que son los de reporte al abrirlos el solo vera incoherencias alfanuméricas por estar encriptados con AES RSA y será ilegible si es abierto con algún editor de texto. Figura 3.13.

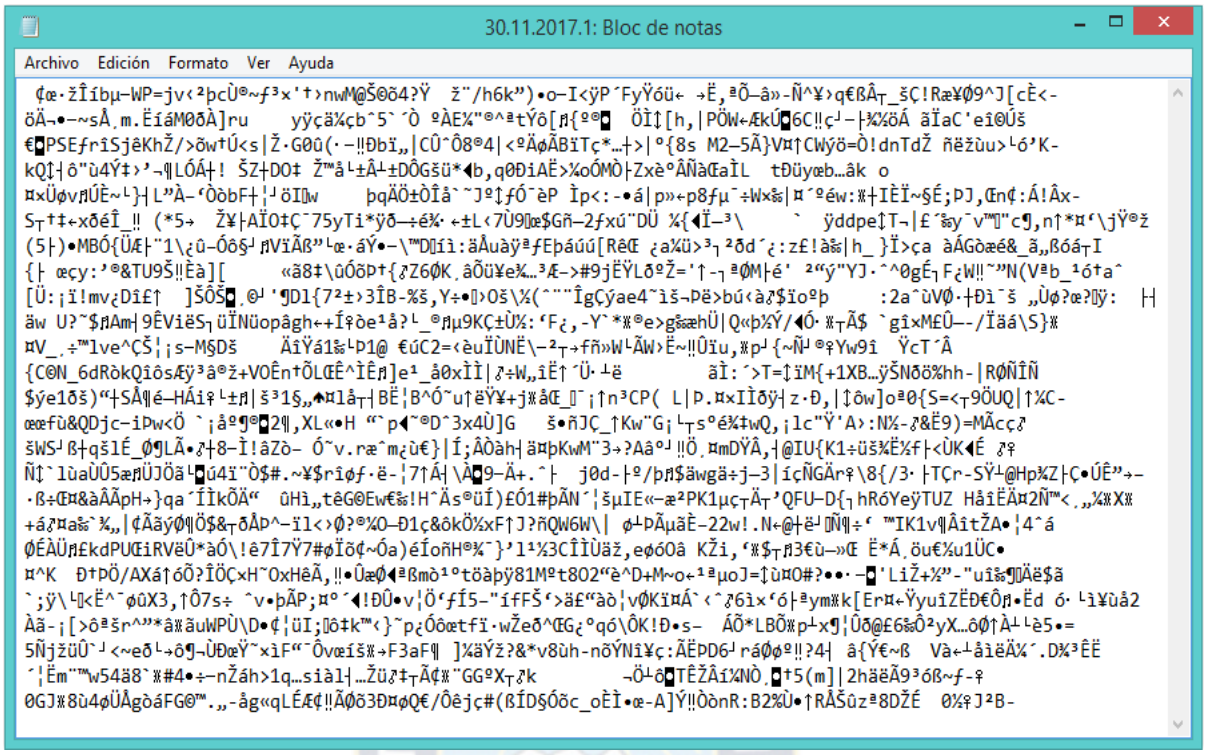


Figura 3. 13: Archivo encriptado con AES RSA

Si por algún motivo el empleado piensa que se está violando su privacidad, no olvidemos que el prototipo guarda las palabras claves en la opción de confidencialidad donde aparecen las palabras y contraseñas escritas en asteriscos al ingresar a sitios confidenciales del empleado como ser correo electrónico, cuentas en bancos, numero de pin de su tarjeta de crédito, etc., . Figura 3.14.

Figura 3. 14: Privacidad de la persona

Por lo tanto se puede concluir que la información recolectada por parte del monitoreo, está encriptado y guardado en el directorio y ruta de instalación de la aplicación.

Por las pruebas obtenidas, se ha podido desarrollar una herramienta que realiza el control y la seguridad de las amenazas informáticas de manera eficaz y eficiente con los reportes detallados para un mayor entendimiento las actividades que realiza el empleado, lo cual responde satisfactoriamente a la hipótesis planteada en la presentación de este trabajo y de manera conjunta, llegando a satisfacer los objetivos planteados en el Capítulo I.

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

En nuestros días, es una necesidad la protección de la información sensible como medida de seguridad obligatoria, debido a la gran cantidad de ataques existentes, si se cuenta entonces de un mecanismo fácil de utilizar, pero a la vez seguro y que no implique gastos adicionales que toda organización pretende resguardar sería de gran utilidad. Al concluir podemos mencionar que los métodos de encriptación que manejan las claves públicas y privadas han pasado a ser una de las grandes áreas de desarrollo de seguridad informática en el mundo de la tecnología actual. Por ese motivo en esta Tesis de Grado se desarrolló un prototipo que permita el acercamiento en el manejo de métodos de encriptación hibrida que es la combinación de el algoritmo de encriptación AES que es simétrico y la encriptación RSA que es asimétrico, el cual se puede destacar su potencial en los problemas matemáticos en los cuales se fundamentan.

Se implementó tres pruebas sobre la aplicación, las cuales mostraron distintos resultados favorables, en la primera prueba se pudo evidenciar que el empleado cumple con normalidad sus funciones, en la segunda prueba el empleado es considerado una amenaza informática por realizar acciones que no están enmarcadas en su trabajo diario y en la tercera prueba el empleado sospecha que es controlado por tal motivo examina el dispositivo móvil

tratando de borrar pruebas que lo incriminen pero se le es difícil por lo que se puede considerar que es un empleado con tendencias a ser una amenaza informática, tomando en cuenta estos diversos factores que podría efectuar el empleado es por el cual el prototipo a llegando a obtener resultados satisfactorios.

Cualquier organización tendría que observar que tan costoso es la información que portan sus empleados concernientes sobre la organización que esté relacionado con los patrimonios y activos, por tal motivo estará más seguro porque sabrá de donde sale la información a terceras personas u organizaciones lo cual implica que recomiende el uso de esta herramienta para un mayor control a cualquier empleado que les parezca una amenaza informática.

4.2 RECOMENDACIONES

Se debe tomar en consideraciones el uso de los algoritmos criptográficos híbridos los cuales son la combinación de simétricos y asimétricos los cuales brindan una mayor seguridad en la encriptación de datos. A continuación se citan algunas recomendaciones para ampliar la misma:

- Expandir los criterios de análisis y búsqueda.
- Unificar la información recolectada en un servidor de la organización.
- Mejorar la inaccesibilidad del empleado a los archivos que contienen los reportes.
- Implementar un nuevo framework como es Ionic, React Native o algún otro para el desarrollo de aplicaciones Android para una mejor vista de la aplicación.
- Se recomienda investigar los nuevos avances de los algoritmos híbridos que presentan más eficiencia y seguridad con el paso del tiempo.

BIBLIOGRAFÍA

Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition, Academic Press*. USA.

Cabrera, E. (2003). *Control.* Recuperado de http://www.monografias.com/trabajos14/control/control.shtml*de los periodistas Derecho español de la información.* Madrid, España: UOC.

Figueroa, B. (2007). *Criterios para evaluar la información.* Recuperado de http://acpon1.ponce.inter.edu/cai/manuales/Evaluacion_Informacion.pdf

Flores, G. (2010). *Comparación y evaluación de algoritmos de encriptación asimétrica y firmas digitales* (Tesis de pregrado). Universidad Mayor de San Andrés, La Paz, Bolivia.

García, Aguinaga y Mora (2000). *Aprenda Linux como si estuviera en primero*. Recuperado de http://www.formacioncontinua.inap.map.es/portal/NuevaWeb/cursos/documentados/Linux.pdf

García, A. y Alegre, M. (2011). *Seguridad Informática.* Madrid, España: Paraninfo.

Grebennikov, N. (2007). *Keyloggers: Qué son y cómo detectarlos.* Recuperado de http://blog.segu-info.com.ar/2007/03/keyloggers-qu-son-y-cmo-detectarlos-i.html

Garrido, A. (2006). *Fundamentos de programación en C++*. Madrid, España: Delta.

Handbook. (1997). *Monitoring and Evaluation as Management Tools.* Recuperado de http://www.policyproyect.com/pubs/advocacy/Spanish/Policy%20Proj%20Sec%20111-8.pdf

Horna, C. (2007). *Seguridad de la Información y Software libre.* Recuperado de http://www.ska-techsite.org/pres/parquesoft.pdf

Herazo, J. (2015). *¿Sabes qué es Cifrado AES 256?* Recuperado de http://liacolombia.com/2015/11/sabes-que-es-cifrado-aes-256/

Liberatori, M. (2006). *Desarrollo de encriptado aes en fpga* (Tesis de pregrado). Universidad Nacional De La Plata, Argentina.

Martínez, F. (2008). *Gestión eficiente de la Información en todo su ciclo de vida.* Recuperado de http://www.revista-ays.com/DocsNum19/Tribuna/Rilo.pdf

Mirabal, A. (2010). *Seguridad en transacciones en línea con tarjeta de débito mediante métodos de encriptación asimétrica hibrida* (Tesis de pregrado). Universidad Mayor de San Andrés, La Paz, Bolivia.

Moreno, M. (2010). *Diseño e implementación de un esquema de encriptación y firmas basado en identidad para dispositivos bug* (Tesis de pregrado). Universidad De Chile Facultad De Ciencias Físicas Y Matemáticas Departamento De Ciencias De La Computación, Chile.

Moya, J. y Escobar, F. (2015). *Desarrollo de una aplicación para encriptar información en la transmisión de datos en un aplicativo de mensajería web* (Tesis de pregrado). Pontificia Universidad Católica Del Ecuador, Ecuador.

Pocho, W. (2009). *Monitoreo de amenazas informáticas para el control de seguridad de los empleados* (Tesis de pregrado). Universidad Mayor de San Andrés, La Paz, Bolivia.

Poratti, G. (2010). *Los próximos 500 años ¿Cómo evolucionaran las casas, computadoras, automóviles, industrias, y robots del futuro?* Argentina: Red Universitaria

Pressman, R. (2002). *Ingeniería del Software*. España: McGraw Hill.

Reig, D. y Vilchez, L. (2013). *Los jóvenes en la era de la hiperconectividad: tendencias, claves y miradas.* Madrid, España: Telefónica Fundación y Fundación Encuentro.

Ribas, J. (2013). *Desarrollo de aplicaciones para Android.* Madrid, España: Anaya-Multimedia

Solomon, B. & Broom (2005). *Computer Forensics JumpStart*. Alameda, USA: Sybex Inc.

Vacca, J. (2002). *Computer Forensics: Computer Crime Scene Investigation.* USA: Charles River Media Inc.

Vásquez, J. (2008). *Consulta y actualización de bases de datos mediante equipos móviles*. Medellín, Colombia: Instituto Tecnológico Metropolitano

WordReference. (15 de octubre de 2016). *Criterio*. Recuperado de http://www.wordreference.com/definicion/criterio

Zorrilla, H. (2016). *La Gerencia del Conocimiento y la Gestión tecnológica.* Recuperado de http://www.wikilearning.com/monografia/la_gerencia_del_conocimiento_y_la_gestión_tecnológica/12224

ANEXOS

ANEXO A

CÓDIGO PENAL DE BOLIVIA
CAPÍTULO XI
DELITOS INFORMATICOS

Artículo 363.-bis (MANIPULACIÓN INFORMÁTICA). El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de un tercero, será sancionado con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días.

Artículo 363.- Ter (ALTERACIÓN ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS). El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o utilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un (1) año o multa hasta doscientos días, (Código Penal, 1999).

ANEXO B

GLOSARIO

Privacidad: se refiere a tener control en el acceso de la información y solo permitirlo a personas autorizadas.

Autenticidad: se refiere a estar seguros de la identidad de una entidad ya sea mensaje, persona, servidor, etc.

Integridad: se refiere a que la información no sea modificada.

Criptografía: es el conjunto de técnicas entre algoritmos y métodos matemáticos que resuelven los problemas de autenticidad, privacidad, integridad y no rechazo en la transmisión de la información.

Cifrar: es la acción que produce un texto ilegible a partir de un texto original.

Texto Cifrado: es un documento que ha sido cifrado.

Descifrar: es la acción inversa de cifrar, es decir, convertir un texto cifrado a otro legible texto original.

Criptografía simétrica: es el conjunto de métodos que permite establecer comunicación cifrada, con la propiedad de ambos lados de la comunicación tienen la misma clave, y ésta es secreta.

Criptografía asimétrica: es el conjunto de métodos que permite establecer comunicación cifrada, donde una de las claves es pública y la otra clave es privada (secreta). Cada usuario tiene un par de claves una pública y otra privada.

Clave privada: es la clave secreta que se usa en la criptografía asimétrica.

Clave pública: es la clave pública conocida, que se usa en la criptografía asimétrica.

Clave simétrica: es la clave secreta que tienen ambos lados de una comunicación en la criptografía simétrica.

Par de claves o llaves: se refiere al par de claves una privada y otra pública usadas en la criptografía asimétrica.

Longitud de la clave o llave: es el número de bits (ceros y unos) que tienen las claves y es solo uno de los parámetros de los que dependen la seguridad de un sistema criptográfico. Actualmente se usan 128 para las claves simétricas. 1024 para el sistema asimétrico RSA.

Cifrado de Bloque: es un sistema criptográfico que cifra de bloque en bloque, usualmente cada bloque es de 128 bits.

DOCUMENTACIÓN

- AVAL PARA LA DEFENZA DE TESIS DE GRADO

M.Sc. Franz Cuevas Quiroz
Docente Tutor Metodológico
Taller de Licenciatura II
Carrera de Informática

- CONFORMIDAD Y AVAL DE TESIS DE GRADO

Lic. Juan Gonzalo Contreras Candia
Docente Asesor
Taller de Licenciatura II
Carrera de Informática

La Paz, 16 de noviembre de 2017

Señor

Lic. Eufren Llanque Quispe

DIRECTOR a.i.

CARRERA DE INFORMÁTICA

FAC. CIENCIAS PURAS Y NATURALES

UNIVERSIDAD MAYOR DE SAN ANDRÉS

Presente

Ref.: AVAL PARA LA DEFENSA DE TESIS DE GRADO

De mi mayor consideración:

Mediante la presente, me dirijo a su Autoridad, en mi calidad de **Tutor Metodológico** para informar que luego de haber realizado el seguimiento de la Tesis de Grado titulado: "**CONTROL Y SEGURIDAD DE LOS EMPLEADOS ANTE AMENAZAS INFORMÁTICAS EN DISPOSITIVOS MÓVILES**", presentado por el Univ. Edwin Gonzalo Mamani Limachi con C.I. 4997781 L.P., para optar al título de **LICENCIATURA EN INFORMÁTICA: MENCIÓN INGENIERÍA DE SISTEMAS INFORMÁTICOS.**

En este sentido, presento mi **conformidad y aval** respectivo para la defensa pública de la Tesis de Grado de acuerdo a Reglamento vigente en la Universidad Mayor de San Andrés.

Sin otro particular, me suscribo con las atenciones más distinguidas.

M.Sc. Franz Cuevas Quiroz

TUTOR METODOLÓGICO

c.c. Arch

La Paz, 16 de noviembre de 2017

Señor

Lic. Eufren Llanque Quispe

DIRECTOR a.i.

CARRERA DE INFORMÁTICA

FAC. CIENCIAS PURAS Y NATURALES

UNIVERSIDAD MAYOR DE SAN ANDRÉS

Presente

Ref.: CONFORMIDAD Y AVAL DE TESIS DE GRADO

De mi mayor consideración:

Tengo a bien dirigirme a su persona, para darle a conocer que luego de efectuar el seguimiento a la estructura y contenido de la Tesis de Grado titulado: "**CONTROL Y SEGURIDAD DE LOS EMPLEADOS ANTE AMENAZAS INFORMÁTICAS EN DISPOSITIVOS MÓVILES**", elaborado por el Universitario: Edwin Gonzalo Mamani Limachi con C.I. 4997781 L.P., en calidad de **Asesor** expreso mi conformidad con el contenido y la forma de trabajo, dando mi **Aval** para que el postulante pueda realizar la defensa de la Tesis de Grado, para optar al título de **LICENCIATURA EN INFORMÁTICA: MENCIÓN INGENIERÍA DE SISTEMAS INFORMÁTICOS,** de acuerdo a normas y reglamento vigentes.

Sin otro particular, me suscribo con las consideraciones más distinguidas.

Lic. Juan Gonzalo Contreras Candia

ASESOR DE TESIS DE GRADO

c.c. Arch