UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

GUÍA DE CONTROLES DE SEGURIDAD PARA DISPOSITIVOS MÓVILES Y ANÁLISIS FORENSE EN LA TELEFONÍA CELULAR

PARA OPTAR AL GRADO DE:

MAESTRO EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

ASESOR:

DOCTOR RUBÉN MAGAÑA

PRESENTADO POR:

ROCIO BELLINY MELGAR FLORES

ALMA YANIRA MENDOZA DELGADO

MAYRA LORENA MOLINA MORÁN

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica

Febrero de 2016

Guía de Controles de Seguridad para Dispositivos Móviles y Análisis Forense en la Telefonía Celular

Rocio Belliny Melgar Flores
e-mail: robellymel@gmail.com
Alma Yanira Mendoza Delgado
e-mail: aymrd14@gmail.com
Mayra Lorena Molina Morán
e-mail: molina.mayra@gmail.com

***Resumen*—** En el presente trabajo se ha realizado una investigación sobre los diferentes controles de seguridad existentes en la actualidad, con el propósito de aportar a las empresas una guía metodológica basada en dichos controles de seguridad específicamente en dispositivos móviles, los cuales están alineados a los tres principales marcos de trabajo de gestión de la seguridad: la metodología de control por objetivos COBIT, la metodología ITIL y las buenas prácticas de las Norma ISO 27001.

Como segunda finalidad en esta investigación, se presenta una propuesta de una guía metodológica para el análisis forense la cual describe el procedimiento para el manejo de la evidencia digital en un proceso judicial bajo la cual esté involucrado un teléfono celular. Finalmente se listan algunas herramientas forenses para teléfonos celulares que pueden servir de apoyo en dicho proceso.

***Palabras clave*—** Controles de Seguridad, Dispositivos Móviles, Evidencia Digital, Herramientas Forenses, Guía de Análisis Forense, Teléfono Celular.

I. INTRODUCCIÓN

El teléfono móvil es uno de los dispositivos electrónicos de mayor uso actualmente. Estos dispositivos que en un inicio fueron creados con el fin de mantener a las personas comunicadas, han ido evolucionando ágilmente en cuanto al desarrollo de su hardware y software, tanto así que realizan actividades similares a las de una minicomputadora, y con una mayor conectividad que un teléfono móvil convencional llegando incluso a reemplazar en algunos casos a una computadora personal. Sin embargo, este avance ha tenido un impacto negativo en el ambiente de control informático, como son los problemas de seguridad y la creación de diferentes tipo de malware, lo cual ha sido propiciada por la gran cantidad de datos personales y de valor que se almacenan en los teléfonos móviles, volviéndose en el punto objetivo para los atacantes.

Es por ello que en el presente trabajo se ha realizado una investigación, la cual está compuesta de la siguiente manera, primeramente se encuentra el marco teórico donde se presenta una breve descripción sobre conceptos básicos relacionados a la evolución de los teléfonos celulares, riesgos de seguridad y delitos informáticos que se dan en los dispositivos móviles, así como también información sobre controles de buenas prácticas basados en estándares internacionales como ITIL, COBIT y la Norma ISO 27001, así como también una descripción sobre las fases que consta el procedimiento de análisis forense.

Posteriormente se presentan dos propuestas de guías, una enfocada a los controles de seguridad para dispositivos móviles y una guía de pasos que se deben llevar a cabo en un proceso de análisis forense. Por último se encuentran algunas conclusiones y recomendaciones obtenidas de dicha investigación y las respectivas referencias.

II. MARCO TEÓRICO

1. DISPOSITIVOS MÓVILES

Un dispositivo móvil de acuerdo a Wikipedia es (mobile device), también conocido como computadora de bolsillo o computadora de mano (palmtop o handheld), es un tipo de computadora de tamaño pequeño, con capacidades de procesamiento, con conexión a Internet , con memoria, diseñado específicamente para una función, pero que pueden llevar a cabo otras funciones más generales.

Ejemplos de dispositivos móviles son: Teléfonos celulares tradicionales, Smart Phones, Computadoras personales de bolsillo, altavoces inalámbricos, GPS, Dispositivos de conectividad inalámbrica como Tablet PC.

En un sentido más amplio se puede decir que es un dispositivo móvil cualquier cosa que pueda estar conectada a una red inalámbrica incluso juguetes, implantes médicos y los cuales cada vez son más accesibles para todo público.

De acuerdo a Overview of Mobile Technology, Journal Online[13], hasta la introducción del Palm Pilot en 1995 los dispositivos móviles eran considerados como planificadores de bolsillo. Hoy en día, tomando rápidamente su lugar en la organización empresarial moderna como una de las herramientas más útiles, sólo superada por sus más poderosos "hermanos", las computadoras de escritorio.

De hecho, muchos de los teléfonos dispositivos móviles están lejos de ser mera periférica y estos dispositivos están siendo utilizados para las funciones que antes podría hacerse en computadoras de escritorio o portátiles. Funciones de negocio tales como correo electrónico, programación,

comunicaciones de voz, procesamiento de texto, incluso emulación de escritorio remoto, de todo se puede hacer en estos dispositivos. Sin embargo, el éxito de esta tecnología tiene un impacto económico significativo en las organizaciones, ya que ahora deben dedicar recursos a la implementación, el control y al mantenimiento de estos dispositivos.

ISACA, Asociación de Profesionales de Auditoría y Control de TI, cuyo significado en inglés es Information System Audit and Control Association, se dedica a la investigación y formación continua de profesionales que se dedican a la Auditoría Interna, Seguridad, Riesgos y Gobierno de Tecnología; a través de su nueva plataforma de conocimiento de seguridad y programa profesional de ISACA denominada CSX Cibersecurity Nexus, publicaron el documento Securing Mobile Devices[12], el cual proporciona lineamientos del uso de dispositivos móviles a nivel de usuario final, responsables de seguridad, departamentos de tecnología de la información, brindando lineamientos de seguridad y auditoria a los dispositivos móviles utilizando Cobit 5.

Los dispositivos móviles tienen un creciente vínculo e interacción a diferentes servicios en la nube y otros dispositivos. El número de teléfonos celulares, asistentes digitales y teléfonos inteligentes ha crecido significativamente en los últimos años, llegando a un alto grado de dependencia de los dispositivos móviles.

El impacto en el uso de dispositivos móviles es visible en dos categorías:

El hardware se ha desarrollado a un nivel en el que la potencia de cálculo y almacenamiento son casi equivalentes a hardware de PC. De conformidad con la Ley de Moore, un teléfono inteligente típico representa el equivalente de lo que solía ser una máquina de gama media de hace una década.

Nuevos servicios móviles han creado nuevos modelos de negocio que están cambiando estructuras organizativas y la sociedad en su conjunto.

La movilidad y accesibilidad han mejorado los negocios y ha permitido a las empresas centrarse en actividades básicas reduciendo el espacio de oficina utilizado. Para los empleados, los dispositivos móviles han traído mayor flexibilidad el “traer su propio dispositivo BYOD”, esto permite que los empleados conecten sus dispositivos e incrementen los riesgos de seguridad, ya que por ser propios sobrepasan las políticas de seguridad de la compañía.

Mientras BYOD puede ser visto como un facilitador, también ha traído una serie de nuevos riesgos, áreas y amenazas asociadas. Estos deben equilibrarse con las ventajas del uso de dispositivos móviles, teniendo en cuenta las necesidades de seguridad de la persona, así como la empresa.

El hecho de que los usuarios se han vuelto más móviles y flexibles ha cambiado drásticamente patrones de trabajo. Hace menos de diez años, la oficina fue el centro de la actividad y requería presencia regular; ahora muchos empleados tienen la libertad de elegir su propio ambiente para trabajar y las horas de trabajo. Esto crea nuevos retos para el área de soporte interno de TI y la contratación de servicios externos. Cuando los usuarios móviles demandan 24/7 horas de servicio, el impacto sobre la estructura y los procesos de la organización es considerable.

Algunos de los riesgos intrínsecos son:

- Aplicaciones populares (apps) como Twitter® o FacebookTM requieren más de diez privilegios críticos en sistemas operativos móviles, incluyendo el cambio de datos, cambiando configuraciones, e iniciar o interrumpir llamadas celulares.
- Registros para más sistemas operativos móviles contienen datos muy detallados. Cuando al dispositivo le ocurren accidentes, se enviarán los datos de las últimas cuatro semanas al proveedor.
- Usuario opt-out es difícil o imposible en un número creciente de aplicaciones móviles. La aplicación se limita a establecer que el usuario necesita algún permiso bastante crítico y no presenta más que un botón "OK".
- La autenticación se efectúa a menudo mediante el número de teléfono móvil (módulo de identidad del abonado [SIM] tarjeta de fichas de una sola vez) y funciones de la aplicación.

El uso de estos dispositivos, también afecta el perímetro de seguridad organizacional, ya que la seguridad se basa en sistemas cerrados controlados por la empresa, esto ha cambiado debido a que los dispositivos de los empleados no están disponibles para actualizaciones, colocación de parches y actualización de medidas de seguridad.

Típicamente, los sistemas abiertos que incorporan dispositivos móviles utilizan servicios en la nube, ya sea para distribución o como estrategia de servicio a los usuarios.

A diferencia de las computadoras más tradicionales portátiles, teléfonos inteligentes y dispositivos similares son generalmente menos transparentes con relación a la actualización de parches del sistema operativo.

Como consecuencia, la gestión de la seguridad tiene que controlar la parametrización de entorno que incluye una serie de incógnitas y debilidades potenciales.

De acuerdo a estudios realizados por CISCO y Google a los que hace referencia el Blog La Fábrica[1], en el año 2016, se utilizara más de 10,000 millones de dispositivos móviles.

Según la publicación de CSX Cibersecurity Nexus, Securing Mobile Devices 2014), los tres grandes riesgos del uso de los dispositivos móviles son: Riesgo Físico, Organizacional y Técnico.

En la Tabla 1 que se muestra a continuación se presenta una breve descripción de los riesgos más frecuentes.

[1] http://lafabricaenlinea.com/dispositivos-moviles/

Vulnerabilidad	Amenaza	Riesgo
La información viaja a través de redes inalámbricas que son a menudo menos seguras que una red cableada.	Externos pueden hacer daño a la empresa.	Intercepción de información, lo que resulta en una violación de datos sensibles, el daño a la reputación de la empresa
La movilidad proporciona a los usuarios la oportunidad de salir de los límites de la empresa, con lo que eliminan muchos de los controles de seguridad.	Los dispositivos móviles se cruzan límites y perímetros de la red, llevando malware, y puede traer este malware en la red de la empresa.	La propagación de malware, que puede dar lugar a la fuga de datos, la corrupción y la falta de disponibilidad de datos necesarios; robo físico
El uso de la Tecnología Bluetooth que es muy conveniente para muchos de los los usuarios, tienen conversaciones de manos libres; sin embargo, a menudo se deja encendido y es entonces detectable.	Los hackers pueden descubrir el dispositivo y luego lanzar un ataque.	La corrupción de dispositivos, la pérdida de datos, llamada intercepción, la posible exposición de información sensible
Información sin cifrar es almacenada en el dispositivo.	En el caso de que un atacante malicioso intercepta datos en tránsito o roba un dispositivo, o si el empleado pierde el dispositivo, los datos se pueden leer y usar.	La exposición de datos sensibles, lo que resulta en daños a la empresa, clientes o empleados
Los datos perdidos pueden afectar la productividad del empleado.	Los dispositivos móviles pueden perderse o ser robados debido a su portabilidad. Los datos sobre estos dispositivos no son siempre sujetos de copia de seguridad.	Los trabajadores dependientes en el móvil, no pueden trabajar en el caso de que se dañe, se pierda o sea robado y los datos que no se hayan respaldado.
La empresa no está administrando el dispositivo	Si hay una estrategia dispositivo móvil, los empleados pueden elegir traer a su cuenta, sin	La fuga de datos, propagación de malware, datos desconocidos la pérdida en caso de pérdida del dispositivo o robo.

Tabla 1. Vulnerabilidades, amenazas y riesgos

La lista mostrada anteriormente no es única, en el apartado dos se listan los riesgos con mayor detalle.

GENERACIONES DE DISPOSITIVOS MÓVILES

Primera (1G) 1973 – 1986. Abril de 1973 Motorola realizo la primera llamada por teléfono móvil del proyecto DynaTAC 8000X, su presentación y comercialización se realizo hasta 1984. El aparato pesaba cerca de un kilo, la primera empresa que proporciono en los Estados Unidos el servicio de de telefonía celular fue Ameritech.

En 1981 Ericson genera el sistema NMT 450 (Nordic Mobile Telephony 450 MHz), este es el primer sistema de telefonía móvil como se conoce a la fecha.

Para 1986 Ericson actualizo el sistema hasta el nivel NMT 900, la nueva versión funcionaba a frecuencias superiores en orden de 900MHz esto facilito el servicio a mas usuarios y avanzar en la portabilidad de los terminales.

Otros sistemas de telefonía móvil desarrollados en los 80 fueron AMPS (Advance Mobile Phone System) y TACS (Total Access Comunication System)

Segunda (2G) 1990. Esta generación nace con los sistemas GSM, IS-136, iDEN e IS-95, se desarrolló la digitalización de las comunicaciones, aumenta el nivel de seguridad, se reduce los costos por la simplificación de la fabricación del terminal.

En esta generación surgen varios estándares de comunicaciones móviles: D-AMPS (EE.UU.), Personal Digital Celular (Japón), cdmaOne (EE.UU. Y Asia) y GSM.

Las operadoras telefónicas implementaron el Acceso Múltiple por División de Tiempo (TDMA) y Acceso Múltiple por División de Código (CDMA) sobre redes Amps surgiendo las redes D-AMPS, siendo esto una ventaja para las telefónicas de migrar de señal analógica a señal digital, sin tener que cambiar el equipo. Con la tecnología digital se inicia la Multiplexión, el poder trasmitir varias llamadas al mismo tiempo a través de un mismo canal.

GSM(Global System for Mobile Communications) este sistema europeo universalizó la telefonía móvil fue el estándar por largo periodo y comenzó a ser insuficiente por la baja velocidad en la transmisión de voz y datos (9.6 Kbit/s) .

Transición (2.5G) 2001 La tecnología 2G incrementa a 2.5G incluyendo los servicios como:

- EMS, mensajería mejorada permite incluir iconos y melodías en los mensajes.
- MMS, mensajería multimedia envía mensajes por medio de GPRS permite insertar imágenes, sonidos, videos y texto. Se incrementa la velocidad de transferencia de datos con las tecnologías GPRS y EDGE.

Tercera (3G) 2002. 3G surge con la necesidad de aumentar la capacidad de transmisión de datos para los servicios de conexión de internet desde la telefonía móvil, realizar teleconferencia, TV y descarga de archivos.

Se desarrolla el sistema tecnológico UMTS (Universal Mobile Telecomunications System) alcanzando velocidades elevadas de 144 kbit/s hasta 7.2 Mbit/s

Cuarta (4G) 2010. En esta generación se eliminan los circuitos de intercambio para emplear las redes de protocolo de internet (IP).

Tecnología que permite acceso a internet con mayor rapidez y ancho de banda, además se inicia la recepción de televisión en alta definición [15].

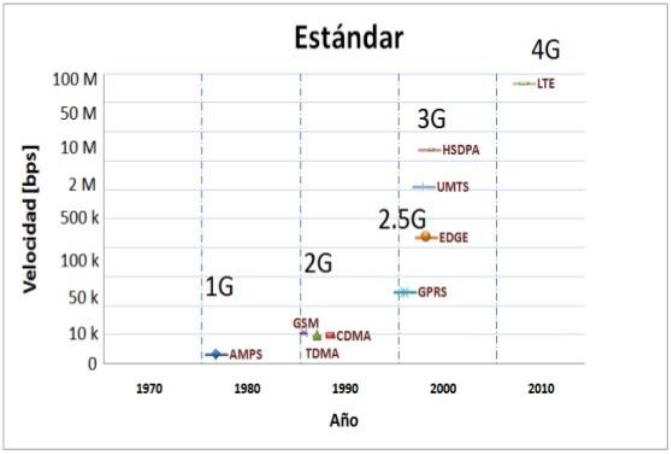

Fig 1. Generaciones de Dispositivos Móviles

Quinta (5G) 2014. Tecnología en proceso de desarrollo, es la sucesora de las redes 4G. Las pruebas realizadas en noviembre 2014 por la compañía Ericsson logro alcanzar velocidades de 5 Gbps reales, las redes 5g se tiene previsto que inicien a implementarse en el año 2018.

TECNOLOGÍAS DE ACCESO EN TELEFONÍA MÓVIL

Las tecnologías de acceso celular se dividen en 2 dos grupos:

1. Sistema Celular Analógico:

   AMPS (Servicio avanzado de telefonía móvil)
   El Sistema Celular Analógico Servicio avanzado de telefonía móvil (AMPS) fue introducido por AT&T liberado en 1983 usaba frecuencias de 800-900 MHZ con un ancho de banda de 30 KHZ para cada canal.

   FDMA (Acceso múltiple por división de frecuencia)
   Acceso múltiple por división de frecuencia (FDMA) Separa el espectro en distintos canales de voz, separando el ancho de banda en pedazos (frecuencias) uniformes.

2. Sistema Celular Digital:

   TDMA
   Este Sistema Celular Digital Acceso múltiple por división de tiempo (TDMA) comprime las conversaciones (digitales) y envía cada una utilizando la señal de radio por un tercio de tiempo solamente. Emplea intervalos de frecuencia entre los 800 y los 1900 MHZ por división de tiempo.

   CDMA
   Tecnologías de acceso celular Acceso múltiple por división de códigos (CDMA) En este sistema después de digitalizar la información, la transmite a través de todo el ancho de banda disponible. Varias llamadas son sobrepuestas en el canal, cada una tiene un código de secuencia único. Posee un ancho de banda de 1.25 MHZ con intervalos de frecuencia de 800 y 1900 MHZ por división de códigos.

   GSM
   La tecnología GSM es el sistema de comunicación más seguro puesto que toda la información que se transmite viaja encriptada por el aire, con nuevos códigos en cada llamada, a la fecha no se han dado casos de ser interceptada y/o reconstruida. Posee un ancho de banda de 200 KHZ. 150 países. Cada vez más avanza en el camino de convertirse en el estándar mundial. El GSM es la tecnología líder a nivel mundial, con más de 380 millones de usuarios.

   GSM es una norma internacional en Europa, Australia y la mayoría de Asia y África. Es un estándar global que ayuda a que los usuarios compren un solo teléfono y lo puedan usar en múltiples países. Para conectarse a los proveedores específicos de servicio en diferentes países, los usuarios de GSM deben simplemente de cambiar tarjetas SIM (SIM cards) cuando viajen de un país a otro país.

Tarjeta SIM
Una de las características principales del estándar GSM es el módulo de identidad del suscriptor, conocida comúnmente como tarjeta SIM. La tarjeta SIM es una tarjeta inteligente desmontable que contiene la información de suscripción del usuario, parámetros de red y directorio telefónico. Esto permite al usuario mantener su información después de cambiar su teléfono. [16]

Paralelamente, el usuario también puede cambiar de operador de telefonía, manteniendo el mismo equipo simplemente cambiando la tarjeta SIM. Algunos operadores introducen un bloqueo para que el teléfono utilice un solo tipo de tarjeta SIM, o sólo una tarjeta SIM emitida por la compañía donde se compró el teléfono, esta práctica se conoce como bloqueo de SIM, y es ilegal en algunos países.

Para acceder a la tarjeta SIM se requiere un número de identificación personal (PIN). Esta es un código de cuatro dígitos, que debe introducirse cuando el teléfono esté encendido. Si un usuario introduce el PIN incorrecto en tres intentos, la tarjeta SIM se bloquea, y la única manera de deshacer esto es entrar los ocho dígitos PUK (Clave de desbloqueo personal). La tarjeta SIM permite diez intentos de hacerse todas las entradas incorrectas, la tarjeta SIM se queda permanentemente bloqueada.

Hay diferentes tipos de tarjetas SIM disponibles:

USIM- Universal Subscriber Identity Module. Este tipo de tarjeta SIM tiene una aplicación que es de tecnología 3G. Contiene la información de los suscriptores, la información de autenticación, y tiene 128KB de almacenamiento dedicado para los contactos.

ISIM–IP IP Multimedia Services Identity Module. Utilizada con un teléfono móvil 3G que opera en la red Tipo de IMS. Contiene información para autenticar el usuario, así como identificarlo.

W-SIM - Willcom SIM. Este tipo de SIM tiene todas las funciones básicas de cualquier tarjeta SIM normal, posee los componentes básicos que conforman un transmisor de teléfono móvil y el receptor ya está integrado en la tarjeta.

RUIM - Re-Usable Identification Module.. Este tipo de SIM es una tarjeta inteligente extraíble que está diseñado para funcionar en teléfonos que funcionan en las redes (CDMA).

HCSIM - High Capacity SIM. Este tipo de SIM posee todas las funciones y características como la de un SIM estándar, pero con una mayor capacidad de almacenamiento.

MSIM - MegaSIM. Este SIM está equipado con una memoria flash de entre 64MB a 1GB. También viene con su propio poder de procesamiento dedicado y una interfaz de alta velocidad.

CAPACIDADES DE ALMACENAMIENTO EN TELEFONÍA MÓVIL

Hace algún tiempo la capacidad de almacenamiento en un teléfono móvil, era algo que no tenía mucha importancia.

Tener más o menos gigas era indiferente debido a que la cantidad de información a almacenar en el smartphone tampoco lo requería. A diferencia hoy en día, las fotos, los vídeos, la música, los juegos y las aplicaciones pueden poner a cero la memoria libre en el teléfono. La opción de usar tarjeta Micro SD es permitida por algunos fabricantes, otros limitan esta alternativa para evitar incompatibilidades, ahorrar problemas técnicos en el terminal, evitar la marginación de la propia memoria interna del teléfono. Por ejemplo algunas marcas venden modelos de 32 GB frente a otros de 16 GB radicando la diferencia está en el almacenamiento y carecen de la opción de adicionar una tarjeta micro SD.

Entre algunas alternativas de almacenamiento externo para los teléfonos móviles están:

- **El almacenamiento en la nube** (*cloud) es una de* las mejores alternativas para solventar esa falta de espacio no sólo en el teléfono móvil, sino también en las Pc's. Aplicaciones en la nube como Dropbox, Box, OneDrive, Google Drive o iCloud ofrecen gigas gratis a los usuarios de las mismas y planes de precio para usar más capacidad si es necesario. Además se tiene la ventaja de poder acceder mediante las aplicaciones móviles al contenido de estas en cualquier momento y lugar.
  Otra ventaja de esta opción es el ahorro financiero y contar con una gran capacidad de gigas gratuitos. Al utilizar esta alternativa hay que tener en cuenta que no conviene descuidar las medidas de seguridad adecuadas para hacer un uso sin riesgos de la nube.
- **Memorias externas**
  Este es un accesorio que amplía la capacidad de memoria de los teléfonos sin que se restrinja a los límites marcados por el fabricante. Existen una amplia gama de productos, los USB duales como el Ultra USB Drive de 64 GB de SanDisk el cual posee doble conector con micro USB permitiendo utilizarlo en cualquier móvil Android o Windows Phone, en iOS también es posible si adquirimos un conector intermedio. Similar se puede hacer con las memorias USB OTG si se tiene el correspondiente adaptador y el móvil permite el uso de esta tecnología.
- **Micro SD**
  Esta opción es sencilla de utilizar, se introduce la tarjeta Micro SD al teléfono y se le indica que utilice la tarjeta SD como almacenamiento para fotos, vídeos o música por defecto a través de las opciones del menú de configuración de cada aparato. También se puede extraer la tarjeta y conectarla a una PC para leer e intercambiar contenidos.
- **Discos Duros o memorias WiFi o Bluetooth** es otra opción para almacenamiento externo se pueden utilizar productos como GoFlex Satellite que además incorpora su propia batería con 10 horas de autonomía.[17]

Fig. 2. Medios de Almacenamiento

2. RIESGOS DE SEGURIDAD EN DISPOSITIVOS MOVILES

RIESGO FÍSICO:

- Particularmente los teléfonos móviles son pequeños por lo que pueden ser fácilmente robados si son principalmente usados en lugares públicos. La pérdida de este dispositivo, es más que haber perdido un aparato, deja expuesto el listado telefónico, las llamadas realizadas, los chats que pueden permitir a un atacante utilizarlos para lograr sus propósitos. Adicionalmente la identidad del propietario queda expuesta.
- Con la intención criminal, los autores pueden ser capaces de recuperar los datos eliminados y una historia del uso del dispositivo móvil.
- Un riesgo significativo adicional es el robo de identidad, que puede ocurrir como resultado de la obtención y el análisis de un dispositivo móvil robado o perdido.
- El vínculo entre el dispositivo y la cuenta a veces está sujeta a un riesgo aún mayor cuando se ofrecen servicios de valor añadido como un add-on para la cuenta de usuario existente. Algunos sistemas operativos pueden ofrecer un repositorio "seguro" para los datos de usuario que van desde la información personal, el almacenamiento automatizado de tarjeta de crédito y la funcionalidad de pago. El riesgo de confiar esos datos sensibles en un dispositivo móvil ("todo en un solo lugar") no debe ser descuidado.

RIESGO ORGANIZACIONAL:

- Actualmente muchos empleados llevan sus propios dispositivos móviles a sus empresas para la ejecución de su trabajo esto se denomina "Bring your own device BYOD", la proliferación de esta situación y los

privilegios que se le otorgan a los diferentes niveles de autoridad para utilizar funciones de la compañía en sus dispositivos móviles es lo que se denomina riesgo organizacional.

- Existen usuarios que tienen privilegios de accesos los cuales transmiten a su propio dispositivo.
- Otro riesgo organizacional importante es la creciente diversidad y complejidad de los dispositivos móviles, ya que los usuarios no comprenden todas las funcionalidades extendidas de sus smartphones.
- Al mismo tiempo, la rápida sucesión de nuevas generaciones de hardware requiere, adaptación constante por parte de los usuarios y empresas.

RIESGO TÉCNICO:

- **Falta de supervisión de la actividad y recuperación de datos.**
  En los dispositivos móviles recientes, los sistemas operativos para simplificar la interfaz del usuario no le permiten modificar la configuración a tan bajo nivel. Lo que deja espacios abiertos para los sypware y malware interceptando los datos en tiempo real que están siendo generados en los dispositivos.

  Los datos objetivos de ataque son:

  - Mensajería: SMS, servicio de mensajes multimedia, recuperar contenido de correos electrónicos, ejecución arbitraria de código vía SMS/MMS, redirigir a través de ataques de Phising usando Hypertext Markup Language.
  - Audio: Iniciar grabado de llamadas, abrir el micrófono para grabar
  - Fotos y video: usar la técnica de piggybacking para obtener las imágenes, tomar y compartir fotos y videos sin dejar rastro.
  - Geolocación: el riesgo es que puede ser monitoreado y obtener a través de GPS la ubicación, incluyendo fecha y estampa de tiempo.
  - Datos estáticos: Lista de contactos, calendario, tareas y notas pueden ser extraídos
  - Datos Históricos: estos pueden ser recuperados y monitoreados en el dispositivo y en el SIM (Llamadas, SMS, contraseñas).
  - Almacenamiento: Los ataques genéricos en un dispositivo de almacenamiento como disco duro o Solid State Disk (SSD).

- **Conexión a red no autorizada**
  La mayoría de Spyware y Malware una vez alojados en un dispositivo móvil requieren un enlace directo entre el atacante y el dispositivo.

- **Pérdida de Datos Sensitivos**
  En este nuevo mundo de negocios y modelos de trabajo es necesaria la disponibilidad de datos de forma descentralizada, los dispositivos móviles usualmente almacenan grandes cantidades de datos e información sensitiva. Por ejemplo, las presentaciones confidenciales usualmente son mostradas en un dispositivo móvil en lugar de una computadora portátil. Este tipo de situaciones incrementa el riesgo de pérdida de datos y con mayor impacto si se trata de información organizacional.

- **Almacenamiento Inseguro de datos sensitivos**
  En la mayoría de dispositivos móviles el Sistema operativo almacena la información de forma cifrada, más sin embargo muchas aplicaciones la almacenan en texto plano y es replicada sin ser cifrada.

- **Transmisión de datos de forma insegura**
  La mayoría de dispositivos móviles utilizan redes inalámbricas para la transmisión de datos, en pocas ocasiones está físicamente conectados a computadoras personales o de escritorio, creando un ambiente inseguro para la transmisión de datos. Usualmente las redes inalámbricas mayormente utilizadas son redes públicas y bluethooth. Los ataques por este tipo de medios son ampliamente conocidos.

- **Usabilidad**
  La usabilidad es un riesgo organizacional importante que se manifiesta de diversas maneras. En algunos casos, el riesgo individual puede ser debido al usuario. En otros casos, la estrategia de los proveedores de hardware y software puede atribuir una mayor prioridad a la comodidad que a la seguridad. Sin embargo, es importante reconocer la usabilidad como un riesgo principal para el uso de dispositivos móviles

3. DELITOS USANDO DISPOSITIVOS MOVILES

Seguridad y riesgos en móviles

De acuerdo al sitio GITS Ciberseguridad[2], según datos de Microsoft del año 2013 (aunque en estudios posteriores en 2014 y 2015 no mejoran los datos):

· El 42% de los internautas está preocupado por los virus informáticos, y menos de la mitad (39%) reconoce activar el cortafuego del equipo. Además, sólo el 46% confirma que tiene instalado un software antivirus en su equipo.

· El 27% están preocupados con los robos de identidad digital y sólo el 38% tiene un PIN (código de identificación personal) para desbloquear el teléfono móvil, mientras que el 32% dice que está al tanto de las últimas medidas de prevención del robo de identidad y el 39% afirma que navega por sitios seguros.

[2]GITS Ciberseguridad.
http://www.gitsinformatica.com/moviles%20seguridad.html

Otro de los más importantes riesgos sigue siendo el Smishing, técnica de estafa similar al Phishing y al Vishing pero a través del teléfono móvil, utilizando un SMS 'gancho' para robar datos. Consiste en el envío de un mensaje corto sms a un usuario indicándole que se ha suscrito a un determinado servicio, y que de no cancelar la suscripción mediante un mensaje corto al número indicado, se le pasará cobrar por el mismo.

En el mensaje de respuesta, se le pueden demandar ciertos datos personales al usuario. La forma de protegerse del smishing es bien sencilla a la vez que obvia. Si usted recibe un mensaje corto que no ha demandado, simplemente bórrelo. Ya sea una solicitud de respuesta, una melodía gratuita o el último logo de moda, lo más sencillo y seguro para su terminal es que borre el sms de la memoria del terminal o de la tarjeta SIM.

Gran parte de la seguridad depende concientización de los usuarios para el uso seguro y adecuado de estas tecnologías.

Recordemos que estos dispositivos también son computadoras, pero más pequeñas y por lo tanto tienen los mismos problemas que sus antecesores.

La tecnología Near Field Communication (NFC) en los celulares, está siendo cada vez más utilizada para realizar compras, reemplazando a la tarjeta de crédito. Esto hace que estos dispositivos sean más atractivos para los criminales.

Según reporte de Norton Cybercrime de Septiembre del 2012[3]:

- 2 de 3 adultos ha sido víctima de cibercrimen.
- La vulnerabilidad de los móviles es 2 veces mayor del 2010 al 2011.
- 31% de los usuarios de móviles han recibido mensajes de texto de un desconocido requiriendo hacer clic a un enlace.
- 35% de adultos han perdido su dispositivo móvil o ha sido robado.
- 2 de 3 adultos no usan aplicativos de seguridad.
- 44% de los adultos no saben que existes aplicativos de seguridad móviles.
- La mayoría de las empresas de antivirus conocidas, actualmente ofrecen aplicativos de seguridad para dispositivos móviles.

De acuerdo a la publicación de Libertad digital [14], nuestros móviles son una puerta abierta para el ciberdelito, el principal problema de los dispositivos móviles es que viven en nuestros bolsos y bolsillos; por lo que es fácil perderlos o que nos lo roben. Los Smartphone disponen de cámaras y sistemas GPS que permiten rastrear nuestra localización. Enviamos emails, hacemos llamadas y enviamos SMS con ellos, almacenamos grandes cantidades de datos personales y económicos, descargamos aplicaciones desarrolladas por desconocidos.

Esta información al igual que en las computadoras personales, puede ser robada a través de malware. Las distintas formas de penetrar en un Smartphone, ya superan a las que se utilizan con los computadores personales. Los Smartphone tienen un puerto USB que nos permite cargarlo.

El cable que utilizamos nos sirve para realizar esta función como para sincronizar datos, lo que pone en peligro nuestra información.

Existen también programas maliciosos que encienden los micrófonos de los *smartphones*, y activan GPS y localización, lo que convierte al dispositivo en una herramienta de vigilancia. Un *malware* instalado en el teléfono puede grabar todas las comunicaciones del dispositivo, leer los correos electrónicos o conseguir credenciales bancarias. Por ejemplo: podría acceder a una cuenta bancaria, dependiendo de la entidad y el portal, cambiar la contraseña, transferir todo el dinero a otra cuenta o incluso cambiar la dirección de email asociada a la cuenta y enviar una copia de la tarjeta de crédito.

4. TENDENCIAS DE SEGURIDAD CIBERNETICA EN EL SALVADOR.

De acuerdo a la publicación de la OEA***, Tendencias de Seguridad Cibernética en Latinoamérica y el Caribe,*** publicado en Junio 2014 [3], El Salvador tiene una población de 6,635,000 , cobertura de internet 25% y suscriptores de banda ancha fija 3.8% hasta junio 2014.

En el país **e**xisten dos ministerios que comparten la responsabilidad de la seguridad cibernética y la prevención del delito cibernético en El Salvador. El Ministerio de Justicia y Seguridad Pública es el líder designado para asuntos de seguridad cibernética, mientras que la responsabilidad de la investigación de cibercrímenes depende principalmente de la Unidad de Delitos Cibernéticos de la Policía Nacional Civil. Este organismo se encuentra actualmente en proceso de convertirse en una nueva Unidad de Delito Cibernético. Se estableció un CIRT nacional, con la sigla SALCERT, y ya está en funcionamiento. Aunque aún no se ha establecido alguna política o estrategia nacional para la seguridad cibernética, ya se encuentra una en proceso de desarrollo. Actualmente, la Policía Nacional Civil está formalizando una asociación con la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) para recibir capacitación relacionada con el delito cibernético a fin de reforzar sus capacidades existentes, desarrolladas, hasta ahora, mediante cursos en línea autodidácticos e interacción informal con autoridades homólogas de la región. Se han implementado mecanismos jurídicos que permiten a la Policía Nacional Civil solicitar la cooperación de empresas privadas cuando se requiera información para combatir el delito cibernético. Sin embargo, en algunos casos la ley exige que estas solicitudes se realicen a través de la Oficina del Fiscal General, responsable de las investigaciones criminales. Actualmente,

[3] http://nowstatic.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

la Presidencia está evaluando la propuesta de una nueva legislación con el nombre de Ley Especial contra los Delitos Informáticos y Conexos. El gobierno emplea una estrategia para la recuperación de datos y la continuidad operacional dentro de sus propias instituciones basada en el uso de dos sitios de almacenamiento remoto en tiempo real, un sitio primario y uno secundario, en los que almacena información de las bases de datos de red. Cuando los datos están almacenados en la computadora de un usuario y no en uno de los dos sitios de almacenamiento remoto, se utiliza software forense para recuperarlos. Dentro de cada institución individual se utilizan firewalls para filtrar paquetes de información maliciosos, con el respaldo del sistema Advance Security de Oracle para seguridad de la base de datos. El acceso externo a través de una VPN (Red Privada Virtual) está protegido por contraseña. Asimismo, el gobierno (persona o entidad del gobierno) manifiesta que se utilizan medidas de seguridad adicionales, no descritas en este documento, de forma rigurosa en todas sus instituciones. Los usuarios individuales reciben un manual de políticas de seguridad cibernética que les provee instrucciones explícitas sobre el uso responsable y autorizado de sistemas de información administrados por el gobierno.

Las autoridades citan una serie de limitantes o brechas para la mejora de la seguridad cibernética y combatir el delito cibernético en El Salvador. Los principales obstáculos son los límites de presupuesto y la falta de soporte de los ISP (proveedores de servicios de Internet) para brindar información acerca de los usuarios sospechosos de haber cometido un delito cibernético. De un modo similar, el gobierno no mantiene relaciones de cooperación con compañías establecidas fuera de El Salvador que proveen servicios de Internet relevantes, tales como proveedores de servicios de correo electrónico, redes sociales o dueños de sitios web. Otras importantes deficiencias identificadas son la falta de un marco de trabajo legislativo integral para combatir el delito cibernético y la necesidad de más capacitación para investigadores y fiscales, además de la necesidad de brindar más oportunidades a los miembros de la Unidad de Delito Cibernético emergente de participar en foros regionales e internacionales de desarrollo de capacidades. Finalmente, las autoridades resaltaron la falta de iniciativas de educación o concientización destinadas a informar mejor a los usuarios de Internet y TIC acerca de los riesgos y buenas prácticas para reducir sus vulnerabilidades. Se ha informado una serie de actividades ilícitas a la Policía Nacional en los últimos años. Las autoridades comunicaron que se abrieron 72 casos de delito cibernético en 2013, que llevaron a 5 condenas. Además, desde la creación de la División de Delitos Cibernéticos en 2011, se documentaron otros 51 casos de pornografía infantil, 26 casos relacionados con amenazas o intimidación, 23 caso de diseminación ilegal de información y 15 casos de acoso sexual. Y mientras que las leyes actuales no penalizan el hackeo como un delito de por sí (aunque en algunos casos se considera una forma de fraude de comunicaciones o violación de medidas de seguridad), las técnicas de hackeo se emplean para ganar acceso no autorizado a cuentas de correo electrónico y redes sociales, lo que sirve de base para cometer otras actividades ilícitas tales como extorsión, diseminación ilegal de información, etc. Sin embargo, dado que las técnicas utilizadas para perpetrar estos últimos delitos no están penalizadas, no hay estadísticas disponibles que permitan evaluar un aumento de uso. En un caso destacable, un depredador sexual estaba contactando víctimas jóvenes a través de redes sociales, ganándose su confianza y luego incitándolos a crear y compartir fotografías y videos sexualmente explícitos. Se alertó a la Policía Nacional y se realizó una investigación que llevó a descubrir evidencia en la computadora del culpable. Luego, por primera vez en El Salvador, se enjuició al individuo y se lo condenó por depredación sexual de menores. A futuro, las autoridades gubernamentales se concentrarán en la sanción de las Leyes Especiales contra Delitos Cibernéticos, la creación de una estrategia y política nacional en materia de seguridad cibernética, y el mayor desarrollo de la capacidad del personal responsable de la administración de incidentes e investigación de cibercrímenes, campañas de concientización y consolidación de las asociaciones internacionales.

5. CONTROLES Y BUENAS PRÁCTICAS EN DISPOSITIVOS MÓVILES (COBIT, ITIL, ISO 27001)

Existen diferentes marcos y buenas prácticas que pueden ser utilizados en las organizaciones para implementar controles que de forma detectiva y preventiva contribuyen a prevenir la materialización de los riesgos antes mencionados

- **COBIT**

Marco de Control utilizado más ampliamente por las empresas multinacionales y que cotizan en bolsa ya que está sumamente ligado al marco de Gobierno Corporativo COSO.

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.

- **ITIL**

ITIL (IT Infrastructure Library, biblioteca de infraestructura de TI) = Marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos.

Como marco de referencia, ITIL se creó como un modelo para la administración de servicios de TI e incluye

información sobre las metas, las actividades generales, las entradas y las salidas de los procesos que se pueden incorporar a las áreas de TI.

- **ISO 27001**

Es la norma ISO de Seguridad de la Información que orienta la creación de un SGSI Sistema de Gestión de Seguridad de la Información. El concepto básico que sustenta el SGSI, es el de Seguridad de la Información. Aunque es un concepto difícil de precisar por todos los elementos que implica, generalmente, se acepta que son tres los componentes de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad.

Esta norma, contiene todo lo requerido para que una organización pueda certificarse.

6. ANÁLISIS FORENSE

Según (Seed Security 2014. Análisis forense y Luis Ángel Gómez. La informática forense, una herramienta para combatir la ciberdelincuencia) El Análisis Forense Digital se define como *"La aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal".* [8,9]

Dichas técnicas incluyen reconstruir el bien informático examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Tal como se define en el concepto anterior, esta disciplina hace uso de tecnología del más alto nivel para poder conservar la integridad de los datos, así también se requiere de una especialización y conocimientos avanzados en materia de informática para poder detectar y examinar cualquier tipo de dispositivo desde una computadora hasta un teléfono celular, el cual puede servir como evidencia en un proceso legal.

Algunos principios básicos que se deben tener en cuenta para realizar un procedimiento de análisis forense son: [10]

1. Esterilidad de los medios informáticos de trabajo.
2. Verificación de las copias en medios informáticos.
3. Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados.
4. Mantenimiento de la cadena de custodia de las evidencia digitales.
5. Informe y presentación de resultados de los análisis de los medios informáticos.
6. Administración del caso realizado.
7. Auditoría de los procedimientos realizados en la investigación.

USOS DE LA INFORMÁTICA FORENSE

Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática forense, entre ellos se puede mencionar: [11]

a) Prosecución Criminal: Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
b) Litigación Civil: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.
c) Investigación de Seguros: La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.
d) Temas corporativos: Puede ser información recolectada en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.
e) Mantenimiento de la ley: La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

El procedimiento de análisis forense en general consta de las siguientes fases [1], tal como se muestra en la Figura 3:

Fig 3. Procedimiento de Análisis Forense

A continuación se describe cada una de las fases de la figura anterior.

1. Adquisición: Acceso al objeto de estudio.

Significa copiar de una manera especial el contenido en bruto de la información del sistema en observación. Luego se trabajará sobre esta copia dejando intacta la información original.

Esta tarea se hará accediendo al dispositivo en modo de sólo lectura para que ni un byte sea alterado desde el momento en que empieza nuestra intervención. Hay que tener en cuenta que el simple arranque del dispositivo que se va a examinar altera algunos archivos en sus contenidos y fechas, varía la cantidad total de archivos, y puede perder credibilidad en un juicio.

2. Preservación: Conservar el objeto.

Este paso incluye la revisión y generación de las imágenes forenses de la evidencia para poder realizar el análisis. Dicha duplicación se realiza utilizando tecnología de punta para poder mantener la integridad de la evidencia y la cadena de custodia que se requiere. Al realizar una imagen forense, nos referimos al proceso que se requiere para generar una copia "bit-a-bit" de todo el disco, el cual permitirá recuperar toda la información contenida y borrada del disco duro. Para evitar la contaminación del disco duro, normalmente se ocupan bloqueadores de escritura de hardware, los cuales evitan el contacto de lectura con el disco, lo que provocaría una alteración no deseada en los medios. Desde este momento ya se pueden efectuar copias exactamente iguales de la imagen para los efectos que diferentes actores puedan conservar una copia de seguridad.

3. Obtención: Análisis y búsqueda.

Es el proceso de aplicar técnicas científicas y analíticas a los medios duplicados por medio del proceso forense para poder encontrar pruebas de ciertas conductas. Se pueden realizar búsquedas de cadenas de caracteres, acciones específicas del o de los usuarios de la máquina como son el uso de dispositivos de USB, búsqueda de archivos específicos, recuperación e identificación de correos electrónicos, recuperación de los últimos sitios visitados, recuperación del caché del navegador de internet, etc.

4. Presentación: Informe de resultados.

Se presenta un informe escrito en un lenguaje técnico y claro y un CD donde se hace accesible al usuario no especializado de una forma ordenada la evidencia recuperada y su interpretación. La documentación se deberá presentar de manera cauta, prudente y discreta al solicitante. La información a entregar deberá ser muy cuidadosa porque se maneja el prestigio técnico según las plataformas y sistemas utilizados.

EVIDENCIA DIGITAL

El Instituto Nacional de tecnologías de la Comunicación de España define la evidencia digital como todos aquellos datos que «de manera digital se encuentran almacenados o fueron transmitidos mediante equipos informáticos y que son recolectados mediante herramientas técnicas especializadas empleadas por un perito en una investigación informática.» Cuya funcionalidad es «servir como prueba física (por encontrarse dentro de un soporte) de carácter intangible (no modificables en las investigaciones informáticas).

En términos sencillos una evidencia digital se refiere a cualquier información que se encuentre en formato digital que pueda establecer una relación entre un delito y su autor.

Para que la evidencia sea aceptada y sirva como soporte en un proceso judicial debe cumplir con los criterios de admisibilidad. Existen cuatro criterios que se deben cumplir para que la evidencia sea admisible, estos son: la autenticidad, confiabilidad, completitud y el apego y respeto por las leyes y reglas del poder judicial.

7. GUÍAS INTERNACIONALES PARA ANÁLISIS FORENSE Y PUBLICACIONES INTERNACIONALES

A continuación en la siguiente tabla se muestra un listado de algunas guías, las cuales son de distribución libre y que tienen un alto reconocimiento a nivel mundial ya que se utilizan para la recolección de evidencias en computación forense [2]:

No	GUÍA	PATROCINADOR
1	RFC 3227 - Guía para recolectar y archivar evidencia	Network Working Group http://www.ietf.org
2	Guía IOCE - Guía de mejores prácticas en el examen forense de tecnología digital	International Organization on Computer Evidence http://www.ioce.org
3	Guía DoJ1 - Investigación en la escena del crimen electrónico	U.S. Department of Justice http://www.usdoj.gov
4	Guía DoJ2 – Examen forense de evidencia digital	U.S. Department of Justice http://www.usdoj.gov
5	Guía Hong Kong Computación forense – Parte 2 – Mejores Practicas	Computación forense – Parte 2 – Mejores Prácticas SWGDE – Scientific Working Group on Digital Evidence http://www.swgde.org/
6	Guía Reino Unido - Guía de Buenas prácticas para evidencia basada en computadoras	ACPO - Association of Chief Police Officers http://www.acpo.police.uk/

Tabla 2. Guías para la recolección de evidencia en computación forense a nivel mundial

Hoy en día existe una diversidad de publicaciones existentes y relacionadas con el tema de análisis forense, algunas de ellas se presentan a continuación:

- **Revista de Información, Tecnología y Sociedad. Informática Forense para Móviles. [18]**

Este artículo proporciona información básica sobre la conservación, adquisición, examen, análisis y presentación de informes de pruebas digitales en los teléfonos celulares, pertinentes para hacer cumplir la ley de respuesta a incidentes y otros tipos de

investigaciones. Esta guía se enfoca en las características de los teléfonos celulares, incluidos los teléfonos inteligentes con funciones avanzadas. Trata de las disposiciones que deben tomarse en cuenta durante el curso de una investigación del incidente. Está definida para atender circunstancias comunes que pueden encontrar el personal de seguridad de las organizaciones y los investigadores policiales, con la participación digital electrónica de datos que se almacenan en los teléfonos celulares y medios de comunicación electrónicos asociados. También complementa sobre el examen y análisis de teléfonos celulares

- **Unificación de Evidencia Digital de Fuentes Dispares (Unification of Digital Evidence from Disparate Sources) (Digital Evidence Bags). [19]**

El trabajo describe un enfoque nuevo en la adquisición y procesamiento de la evidencia digital adquirida de los dispositivos y fuentes digitales. Hasta la fecha, la captura de la evidencia digital se ha efectuado desde el dispositivo de origen y los diferentes métodos y depósitos (tipos de archivos) utilizando en diferentes tipos de dispositivos digitales (por ejemplo, ordenador, PDA, teléfono móvil). Este documento detalla un nuevo enfoque llamado Evidencia digital Bolsa (DE B) propone un contenedor universal para la captura de la evidencia digital. El concepto de la evidencia digital propone utilizarse para la racionalización de captura de datos y permitir que múltiples fuentes de evidencia puedan ser procesados en un entorno multiprocesador distribuido y maximizando así el uso del poder de procesamiento disponible. La orientación descrita en este trabajo especifica el proceso forense para extenderse más allá de la captura forense estática tradicional de la evidencia en la captura en tiempo real "en vivo" de la evidencia. La Bolsa para pruebas digital se puede utilizar para proporcionar una pista de auditoría de los procesos llevados a cabo en las pruebas, así como la verificación de la integridad.

- **Sistema Forence GSM para Telefonía Móvil (Forensics and the GSM Mobile Telephone System). [20]**

El sistema GSM es el sistema más popular para la comunicación móvil en el mundo. Los delincuentes suelen utilizar los teléfonos GSM y por lo cual es necesario que los investigadores forenses se enfoquen que la evidencia puede obtenerse a partir del sistema GSM. El documento explica los conceptos básicos del sistema GSM. Elementos de las pruebas que se pueden obtener desde el equipo móvil, la tarjeta SIM y la exploración de la red central. La existencia de herramientas para extraer las pruebas y componentes del sistema, crean la necesidad de desarrollar procedimientos y herramientas forenses más sólidas para la extracción de tales pruebas. El documento concluye con una presentación sobre el sistema UMTS futuros, que se basa en gran parte en el diseño de GSM.

- **Proceso para el Desarrollo de Examen en Pruebas de Teléfono Celular (Developing Process For The Examination Of Cellular Phone Evidence). [21]**

Debido a que los requerimientos la extracción de datos de los teléfonos celulares es variada, al igual que las técnicas utilizadas para procesarlos. Y en otros casos es necesario un examen forense completo y una recuperación de datos borrados, extracción del sistema de archivos integrado y la memoria física. Estos factores hacen aumentar la importancia de la elaboración de las reglas y procedimientos para la extracción y la documentación de los datos de los teléfonos celulares. Este artículo presenta un resumen de las consideraciones del proceso para la extracción y la documentación de los datos del teléfono celular.

- **Análisis Forense de Teléfonos Móviles (Mobile Phone Forensic Analysis).[22]**

Debido al crecimiento acelerado en el uso y la dependencia de los teléfonos móviles surgen rápidamente las actualizaciones y avances tecnológicos en los mismos, al igual que el desarrollo de teléfonos inteligentes. La explotación de esta demanda ha generado los problemas como el fraude, uso criminal y robo de identidad que han llevado a la necesidad del análisis forense para el teléfono móvil. Este documento plantea el análisis forense en el teléfono móvil, lo que significa, uso de la misma y las herramientas de software utilizadas.

- **Forense y Tarjetas SIM, Descripción General (Forensics and SIM cards: an Overview). [23]**

El trabajo presenta la construcción de una herramienta para la parte de recolección de evidencia (creación de la imagen). Aporta información referente a los fundamentos de sistemas de archivos que se encuentran en las tarjetas, toda esa información se utilizada para crear un algoritmo y programarlo en lenguaje C estándar.

- **Estudio y Análisis de Evidencia Digital en Teléfonos Celulares con Tecnología GSM para Procesos Judiciales.[24]**

El análisis permite obtener evidencias o pruebas auténticas e íntegras, que ayudan a la investigación en un proceso judicial, para ser posteriormente alidadas para e l mismo. Este trabajo presenta cuales evidencias digitales potenciales puede ser proporcionada por el teléfono móvil, para lo cual se analiza la información del Equipo y

la Tarjeta SIM. Este análisis se desarrolla en base a estudios de investigadores nacionales, que han trabajado en el desarrollo de procedimientos para la validación de evidencia digital, y organismos internacionales que han desarrollado herramientas forenses especializadas en hardware y software, que ayudan a encontrar evidencia y analizarla para procesos judiciales

Publicaciones del NIST. (National Institute of Standards and Technology)

- **Directrices sobre análisis forense de dispositivos móviles (Guidelines on Mobile Device Forensics) (NIST Special Publication 800-101). [25]**

Esta guía presenta un estudio profundo en los dispositivos móviles y explica las tecnologías involucradas y su relación con los procedimientos forenses. El documento considera los dispositivos móviles con características superiores a las capacidades de comunicación de voz y mensajes de texto. La guía contiene procedimientos para la convalidación, conservación, adquisición, exploración, análisis y reporte de la información digital.

- **Herramientas Forenses para Teléfonos Móviles (Cell Phone Forensic Tools: An Overview and Analysis Update) (NISTIR 7387). [26]**

Este informe provee una visión general de las actuales herramientas diseñadas para la adquisición, el examen y la presentación de informes de la información obtenida en dispositivos móviles, además plantea la comprensión de sus capacidades y limitaciones. Es continuación de NISTIR 7250 de las Herramientas forenses para teléfono celular, la cual se orienta en presentar cambios que han sufrido las herramientas forenses, presenta nuevas herramientas que no fueron reportadas anteriormente manteniendo la estructura de trabajo que apoya el análisis forense. El documento 7250 brinda una visión de las herramientas de software forense diseñadas para la adquisición, análisis, y reporte de datos almacenados en dispositivos móviles. La publicación muestra un estudio general sobre las capacidades y limitaciones para cada herramienta en detalle a través de una metodología basada en diferentes escenarios.

III. LEGISLACIÓN EN EL SALVADOR PARA EL USO DE DISPOSITIVOS MÓVILES EN LOS SERVICIOS FINANCIEROS

El día 5 de enero de 2014, fue publicada en la página web de El Diario de Hoy, la noticia con el título **"BCR definirá legislación para servicios financieros móviles"**[4]**,** la cual se refiere a la iniciativa de regular en el país, el uso de los dispositivos móviles específicamente en los servicios financieros.

En la propuesta se establece que aquellas instituciones o empresas que quieran prestar el servicio de banca móvil deberán, primero, crear una nueva entidad, y será ésta la que se someterá a todo el proceso de autorización ante el regulador.

Entre los principales servicios móviles que se ofrecen en el país está el de Tigo Money ofrecido por una compañía privada de telefonía que actualmente opera en El Salvador. Otro punto de enfoque es asegurar que se cumplan las condiciones mínimas de seguridad, sobre todo en relación a las aplicaciones móviles (Apps), su diseño y que cada una de las transacciones que se realice bajo los estándares globales.

"Los temas relacionados con la seguridad y la protección del usuario en cada transferencia monetaria también son parte de la propuesta. Cada aplicación debe ajustarse a estos criterios", así lo menciona la noticia publicada en la edición electrónica de El Diario de Hoy en la fecha ante mencionada.

Así también se tiene de referencia que en el mes de agosto del año 2015, se aprobó en El Salvador la **"LEY PARA FACILITAR LA INCLUSION FINANCIERA",** la cual tiene por objeto propiciar la inclusión financiera, fomentar la competencia en el sistema financiero, así como reducir costos para los usuarios y clientes del referido sistema, estableciendo las regulaciones que deben seguir las empresas que se dedican a realizar negocios con dinero electrónico.

Las Sociedades Proveedoras de Dinero Electrónico, son sociedades anónimas de capital fijo; su finalidad se limitará a la de proveer dinero electrónico; pero también podrán administrar u operar sistemas de pagos móviles; es decir, compensar y liquidar pagos entre los proveedores de dinero electrónico, con la autorización del Banco Central de Reserva de El Salvador, y observando los requisitos establecidos por éste para tal efecto.

Entre las obligaciones de las referidas sociedades contenidas en la Ley indica que estas estarán obligadas a contar con personal, equipo, plataforma tecnológica para administrar el dinero electrónico, sistemas de control administrativo, aplicaciones de seguridad, plan de negocios, manuales, procedimientos, políticas, controles internos y planes de continuidad del negocio que garanticen el adecuado funcionamiento para ofrecer los servicios regulados en esta ley, todo de conformidad al ordenamiento jurídico vigente, a las Normas Técnicas que el Banco Central dicte para tal efecto, por medio de su Comité de Normas, y a las disposiciones de la Unidad de Investigación Financiera de la Fiscalía General de la República, en materia de prevención de lavado de dinero y de activos y financiamiento al terrorismo; por tanto, las Sociedades Proveedoras serán consideradas como sujetos obligados de acuerdo al artículo 2 de la Ley Contra el Lavado de Dinero y de Activos. Los bancos, los bancos cooperativos, y las sociedades de ahorro y crédito

[4] http://www.elsalvador.com/articulo/negocios/bcr-definira-legislacion-para-servicios-financieros-moviles-48008

quedan facultados para proveer dinero electrónico, para lo cual deberán cumplir con las disposiciones de esta ley que les sean aplicables. La Superintendencia verificará el cumplimiento de las disposiciones de esta ley y de la normativa técnica que se emita, previo a la prestación del servicio

El Articulo 9 de esta Ley incluye el tema de Protección de datos, el cual dice lo siguiente: "La información de los clientes y de sus operaciones, realizadas de conformidad con esta ley, es confidencial y deberá darse a conocer únicamente al titular, al Banco Central, a la Superintendencia, a la Dirección General de Impuestos Internos cuando estos lo requieran para el ejercicio de sus funciones, ya sea en un proceso de fiscalización o supervisión, y a las autoridades respectivas para el esclarecimiento de delitos".

El Artículo 14 dicta lo siguiente: "Las Sociedades Proveedoras de Dinero Electrónico podrán solicitar al Banco Central que les autorice para ser administradores de sistemas de pagos móviles, siempre que cumplan lo que el Banco Central disponga, de conformidad a su Ley Orgánica en lo referente a los sistemas de pagos.

Los administradores de pagos móviles serán autorizados para operar sistemas o plataformas tecnológicas que permitan pagos o transferencias de dinero, principalmente dinero electrónico, entre productos de diferentes instituciones financieras e independientemente del operador de telefonía móvil con que cuente el cliente.

De acuerdo a lo mencionado en la ley, el uso de dispositivos móviles, en particular los teléfonos móviles, se incrementará para la realización de transacciones financieras, motivo por el cual consideramos importante la disponibilidad de guías de seguridad que prevengan la materialización de los riesgos a los que se exponen estos dispositivos y en el caso de materializarse también es de suma importancia la disponibilidad de una guía que permita llevar a cabo el procedimiento de análisis forense en estos dispositivos de manera ordenada y legal.

IV. PRÁCTICAS ACTUALES DE INVESTIGACIÓN FORENSE DE DISPOSITIVOS MÓVILES EN EL SALVADOR

En este apartado se pretende dar a conocer el manejo y tratamiento que se le da actualmente en El Salvador, a los dispositivos móviles cuando son utilizados como evidencia de un delito de cualquier índole, por medio de las instituciones encargadas para llevar a cabo dicho proceso, para ello se realizó una entrevista a la Jefa de la Unidad de Vida de la Fiscalía General de la República de El Salvador (Para conocer el detalle completo de la entrevista ver el apartado de Anexos).

En dicha entrevista nos comentaban que los dispositivos móviles son considerados como una evidencia importante en el caso de delitos, por ejemplo cuando ocurren casos de homicidios y se encuentra el teléfono de la víctima, este se recolecta como evidencia pues ahí se encuentra plasmado las ultimas llamadas y mensajes de texto realizados por la víctima, nombre de la persona que llamó, entre otra información que puede ser importante. Luego de ser recolectado como evidencia se procede a realizar el análisis forense y este se canaliza a través de la unidad de Análisis de la misma institución.

En la Unidad de Análisis de la Fiscalía General de la República, se cuenta con personal con conocimientos técnicos para poder realizar análisis forense en los dispositivos electrónicos, el cual consiste en el vaciado de información de dichos dispositivos, pero ya para materializarlo para un proceso legal, lo ideal y conveniente es que este se haga a través de la Policía Nacional Civil (PNC), por medio de su Unidad de Análisis, pues puede generar cierto conflicto, en el sentido de decir que el mismo ente está recolectando y produciendo pruebas, por eso es mejor hacer uso de la Unidad de Análisis de la PNC, ya que es la encargada de realizar estos tipos de análisis, además dicha institución (PNC) cuenta con sus propios peritos reconocidos y especializados para realizar estos análisis, mientras que la Fiscalía no cuenta con peritos acreditados para este proceso, debido a que puede generar conflicto de intereses.

En la Unidad de Análisis y Tratamiento de la Información de la Fiscalía General de la República se cuenta con dispositivos especiales para la extracción de información, tal es el caso de un dispositivo llamado **UFED** con el que cuentan para la extracción de información y también cuentan con un programa llamado **I2**, el cual permite procesar la bitácora de llamadas, generar gráficos y hacer una línea de tiempo, frecuencia de llamadas, con solo conocer el número del teléfono que está sirviendo como evidencia. (Para mayor información sobre las herramientas UFED e I2, la podrá encontrar en el apartado de Clasificación de Herramientas para Análisis Forense en Teléfonos Celulares)

Para que una prueba sea catalogada como evidencia válida en un proceso legal se debe seguir y respetar la cadena de custodia, que no es más que el aseguramiento de la evidencia, es decir que la evidencia que se recolectó al inicio en la escena del delito sea la misma que se presente en un juicio, sin presentar alteración alguna. La cadena de custodia permite asegurar que cierta evidencia o información viene de un teléfono específico.

Según la información recopilada en la Unidad de Vida de la FGR el proceso de la cadena de custodia inicia cuando el perito de la Policía Técnica Científica recibe el teléfono de mano del técnico de laboratorio y se entrega en la escena, esta secuencia debe ser documentada, actualmente se utiliza una hoja de reporte de la cadena de custodia, donde queda registrado quien recolecta la evidencia, de donde se recolecta, lugar, fecha y hora del delito, nombre de la víctima, a quien se entrega la evidencia, entre otros datos importantes para ser documentado posteriormente en un acta, la cual debe ser presentada en el juicio.

Hay que tener en cuenta que la recolección de evidencia debe estar a cargo de un técnico de la PNC, la Fiscalía realiza el vaciado de la información y la PNC el análisis y el peritaje.

Actualmente la FGR cuenta con acuerdos con las empresas operadoras de telefonía móvil en el país (Según acuerdo 285 del documento de Decretos Legislativos, diario oficial No. 51 del tomo 386 de la Ley Especial para la Intervención de la Telecomunicaciones emitida el 18/02/2010, esta ley establece la intervención de las telecomunicaciones como instrumento útil en la persecución del delito, en particular la criminalidad organizada, estando su utilización resguardad por garantías que eviten abusos contra la intimidad de las personas) , quienes brindan cierto tipo de información que es solicitada tal como la bitácora de llamadas, mensajes de texto, llamadas, hora, fecha, aunque se ha dado el caso que dicha información a veces no es verídica, pues el chip está a nombre de otra persona y no del sospechoso, también se dan casos de clonación de chips, que consiste en reactivar un chip que ha sido bloqueado.

En la entrevista se pudo conocer que la Fiscalía General de la República como la Policía Nacional Civil realizan un papel muy importante en el proceso de recolección y análisis de la evidencia, en cuanto a teléfonos celulares ser refiere, para ser utilizados como instrumento de prueba y que sirva como una evidencia válida para ser presentada en un juicio en el caso de un delito de cualquier índole, así también se pudo conocer que en nuestro país, se tiene establecido un proceso que involucra herramientas informáticas para realizar el análisis forense de dichos dispositivos móviles.

V. PROPUESTA DE GUÍA DE CONTROLES DE SEGURIDAD PARA DISPOSITIVOS MÓVILES

De acuerdo a lo expuesto en el marco teórico, consideramos importante diseñar una guía que permita a las compañías que actualmente se están innovando tecnológicamente con el uso de dispositivos móviles como herramientas de trabajo para sus empleados.

Para la elaboración de dicha guía hemos tomado como referencia el Marco de Gobierno de TI COBIT5[6], Procesos Catalizadores COBIT5[7], ITIL[5] y la Norma ISO/IEC270001:2005[4].

Dadas las condiciones, amenazas y vulnerabilidades a las que se encuentran expuestas las compañías que están innovando para prestar mejores servicios y permiten que sus empleados lleven sus propios dispositivos (BYOD) a su trabajo o realicen su trabajo a través de ellos; y dado que en El Salvador ya contamos con una Ley que regula la inclusión financiera la cual contiene los requerimientos de seguridad que deben cumplir las instituciones que los presten; consideramos importante proporcionar una guía que les permita marcar una ruta de seguridad desde la gobernanza en el uso de la tecnología móvil hasta el establecimiento de controles a nivel operativo.

Inicialmente para plantear una guía de controles de seguridad es recomendable identificar qué tipo de dispositivo móvil se está utilizando y clasificar el nivel de riesgo al que se está expuesto y definir niveles de tratamiento de los datos y la información.

Los principales pasos a seguir que recomendamos son:

a) Establecer un gobierno en el uso de los dispositivos móviles

Mostramos a continuación como los diferentes modelos de referencia de buenas prácticas definen el modelo de gobernabilidad:

- **Cobit 5**

A través de sus procesos habilitadores, denominados EDM guía a las empresas a evaluar el sistema de gobierno, orientarlo hacia el cumplimiento de los principios y modelos para toma de decisiones, supervisarlo a través de mediciones para identificar si el uso de dispositivos móviles les agrega el valor requerido.

EDM01.01 Evaluar el sistema de gobierno.
Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de TI de la empresa.

EDM01.02. Orientar el sistema de gobierno.
Informar a los líderes y obtener su apoyo, su aceptación y su compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios, modelos para la toma de decisiones y niveles de autoridad diseñados para el gobierno. Definir la información necesaria para una toma de decisiones informadas. Este proceso habilitador proporciona un ambiente positivo en relación a la cultura y ambiente de seguridad de la información, la cual se traslada al propietario del dispositivo móvil.

EDM01.03 Supervisar el sistema de gobierno.
Supervisar la ejecución y la efectividad del gobierno de TI de la empresa. Analizar si el sistema de gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI. Permite alinear la política de uso de dispositivos móviles y estándar de seguridad a las legislaciones y regulaciones.

EDM02.01 Evaluar la optimización de valor.
Evaluar continuamente las inversiones, servicios y activos del portafolio de TI para determinar la probabilidad de alcanzar los objetivos de la empresa y aportar valor a un coste razonable. Identificar y juzgar cualquier cambio en la dirección que necesita ser dada a la gestión para optimizar la creación de valor. En relación a los dispositivos móviles permite identificar las necesidades de los usuarios y del negocio de uso de dispositivos móviles.

EDM02.02 Orientar la optimización del valor.
Orientar los principios y las prácticas de gestión de valor para posibilitar la realización del valor óptimo de las inversiones TI a lo largo de todo su ciclo de vida económico. Establecer medidas financieras y no financieras para describir el valor agregado del uso de dispositivos móviles.

- **ISO/IEC27001:2005**

La Norma ISO/IEC27001:2005 En la tabla A.1 Objetivos de Control y Controles. A.6 Aspectos organizativos de la seguridad de la información, define los controles, que orientan a la creación de un Comité de Seguridad, el cual debe contar con el total apoyo de la Dirección, refiérase a la Alta Administración de la compañía, siendo estos los siguientes:

A6.1.1 Comité de Gestión de la Seguridad de la información. La Dirección debe prestar un apoyo activo a la seguridad dentro de la organización a través de directrices claras, un compromiso demostrado, asignaciones explicitas y el reconocimiento de las responsabilidades de seguridad de la información.

A.61.4 Provisión de autorización de recursos para el proceso de la información. Para cada nuevo recurso de procesado de la información, debe definirse e implantarse un proceso de autorización por parte de la Dirección.

A.6.1.5 Acuerdos de confidencialidad. Debe determinarse y revisarse periódicamente la necesidad de establecer acuerdos de confidencialidad o no revelación, que reflejen las necesidades de la organización para la protección de la información.

- **ITIL**

Si bien este marco de referencia, no es tan amplio como los antes mencionados toma como referencia la norma ISO/IEC 38500, para mencionar la importancia de definir un gobierno, que incluye reglas, políticas y procesos o leyes por las cuales se rige la compañía. La versión 3 de ITIL Service Strategy SS, define la gobernanza en tres actividades:

Evaluar
Esto se refiere a la evaluación continua del desempeño de la organización y su entorno. Esta evaluación incluirá un conocimiento íntimo de la industria, sus tendencias, entorno regulatorio y los mercados a los que la organización sirve.

Los productos que se utilizan para evaluar la organización podrían incluir:

- Rendimiento financiero
- Carteras de servicios y de proyectos
- Las operaciones en curso
- Oportunidades y amenazas
- Las propuestas de los gerentes, accionistas, clientes, etc.
- Contratos
- La retroalimentación de los usuarios, clientes y socios.

Dirigir
Esta actividad se refiere a la comunicación de la estrategia, políticas y planes a través de la administración. Ello También asegura que se den las directrices apropiadas para poder cumplir con el gobierno.

Esta actividad incluye:

- La delegación de autoridad y responsabilidad
- Comités de dirección para comunicarse con gestión, y para discutir la retroalimentación (también utilizada durante 'evaluar')
- Comunicación de visión, estrategias y políticas a los directivos, para su conocimiento y que se espera para cumplir con ellos
- Las decisiones que se han intensificado hasta la gestión, o donde el gobierno no está claro.

Monitorizar
En esta actividad, los gobernadores de la organización son capaces de determinar si el gobierno está siendo cumplido con eficacia, y si los hay excepciones. Esto les permite tomar medidas para rectificar la situación, y también proporciona entrada evaluar aún más la eficacia de la corriente medidas de gobierno.

Para ejecutarlo se requiere lo siguiente:

- Un sistema de medición
- Indicadores clave de rendimiento
- Evaluación de riesgos
- Auditoría de cumplimiento
- Análisis de capacidad, que se asegurará de que la gestión tiene lo que necesitan para cumplir el gobierno corporativo.

b) Identificar qué tipo de dispositivos se utilizaran en la compañía.

A continuación presentamos la siguiente tabla que puede ayudar como guía a la identificación de los dispositivos móviles que se utilizaran en la compañía y la cual puede variar de acuerdo al crecimiento constante de la tecnología.

Categoría	Dispositivos	Ejemplos
1	El almacenamiento de datos (limitado), servicios de telefonía básica y mensajería, sistema operativo propietario (limitada), sin capacidad de procesamiento de datos.	Teléfonos celulares tradicionales.
2	El almacenamiento de datos (incluyendo externo) y capacidad de procesamiento de datos, OS estandarizado (configurable), servicios extendidos.	Smartphones Dispositivos de bolsillo
3	Capacidad de almacenamiento de datos, procesamiento y transmisión a través de canales alternativos, la conexión a Internet de banda ancha, OS estandarizada, capacidades tipo PC (configurable)	Smartphones avanzados Tablet PC
4	Comunicación con Automóviles, dispositivos implantados en el cuerpo humano.	Sincronización de un dispositivo móvil con el auto, uso de manos libres.

Tabla 3. Categorías de Riesgo de Dispositivos Móviles

c) Realizar un análisis de riesgo e impacto.

Posteriormente, es recomendado identificar qué nivel de impacto tendrían en relación a los tipos de riesgo identificados: Riesgo Físico, Riesgo Operacional y Riesgo Técnico.

Riesgo	Categoría 1	Categoría 2	Categoría 3	Categoría 4
Físico				
Hurto	Bajo	Medio	Alto	Alto
Perdida	Medio	Medio	Medio	Medio
Daño/Destrucción	Alto	Alto	Bajo	Bajo
Organizacional				
Aglomeración / usuarios pesados	Bajo	Bajo	Alto	Alto
Complejidad/Diversidad	Bajo	Medio	Alto	Alto
Técnico				
Monitoreo de la actividad, recuperación de datos	Bajo	Alto	Alto	Alto
Conectividad de red no autorizada	Bajo	Medio	Alto	Alto
Vista Web / suplantación	Bajo	Medio	Alto	Alto
Fuga de datos sensibles	Bajo	Alto	Alto	Alto
Almacenamiento de datos sensibles en condiciones de riesgo	Medio	Alto	Medio	Medio
Transmisión de datos sensibles en condiciones de riesgo	Bajo	Alto	Medio	Alto
Manejo de Vulnerabilidades	Bajo	Alto	Alto	Alto
Usabilidad	Bajo	Bajo	Alto	Alto

Tabla 4. Categoría de Dispositivos móviles e impacto por riesgo

Los marcos de referencia de buenas prácticas también lo incluyen.

- **Cobit 5**

A través de los procesos habilitadores evalúa, orienta y supervisa la gestión de los riesgos. Estos procesos habilitadores están relacionados a la norma ISO/IC 3100 Marco de Referencia para la Gestión de Riesgos.

EDM03.01 Evaluar la gestión de riesgos.
Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado y definir los riesgos clave para el uso de dispositivos móviles.

EDM03.02 Orientar la gestión de riesgos.
Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo. Alinear los estándares de seguridad de dispositivos móviles con la política de administración de riesgos.

EDM03.03 Supervisar la gestión de riesgos.
Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución. Tomar acciones de remediación para mitigar riesgos específicos para dispositivos móviles.

- **ISO/IEC27001:2005**

La Norma ISO/IEC27001:2005, define los requisitos necesarios para la creación de un Sistema de Gestión de Seguridad de la Información (SGSI).

El numeral 4. Sistema de Gestión de la Seguridad de la Información, 4.2 Creación y gestión del SGSI, los literales a) al b) definen los pasos a seguir para definir el alcance y límites de un SGSI, la política de SGSI y generalidades de su contenido y del literal c) al h) especifica lo siguiente en relación a los riesgos.

c) Definir el enfoque de la evaluación de riesgos de la organización

1. Especificar una metodología de evaluación de riesgos adecuada para el SGSI, las necesidades de negocio identificadas en materia de seguridad de la información de la empresa y los requisitos legales reglamentarios.
2. Desarrollar criterios de aceptación de riesgo y fijar los niveles de riesgo aceptables. La metodología seleccionada para la evaluación de riesgos debe asegurar que las evaluaciones de riesgos generen resultados comparables y reproducibles.

d) Identificar los riesgos

1. Identificar los activos que están dentro del ámbito de aplicación del SGSI y a los propietarios de estos activos
2. Identificar amenazas a que están expuestos los activos
3. Identificar vulnerabilidades bajo las que podrían actuar dichas amenazas
4. Identificar los impactos que sobre los activos puede tener una pérdida de confidencialidad, integridad y disponibilidad de los mismos.

e) Analizar y valorar los riesgos

1. Evaluar los efectos de la actividad empresarial de la organización que pudieran derivarse de eventuales fallos de seguridad, teniendo en cuenta las consecuencias de una perdida de confidencialidad, integridad o disponibilidad de los activos.
2. Evaluar la probabilidad, de una forma realista, de que se produzcan fallos de seguridad, teniendo en cuenta las consecuencias de una perdida de confidencialidad, integridad o disponibilidad de los activos.
3. Estimar los niveles de riesgo.
4. Determinar si los riesgos son aceptables o si requieren un tratamiento conforme a los criterios de aceptación de riesgos establecidos.

f) Identificar y evaluar las opciones para el tratamiento de riesgos.

Las posibles acciones a realizar, entre otras, son las siguientes:

1. Aplicar controles adecuados
2. Asumir los riesgos de manera consciente y objetiva, conforme a las políticas de la organización y a los criterios de aceptación de riesgos
3. Evitar los riesgos
4. Transferir los riesgos asociados a la actividad empresarial a otras partes, como por ejemplo compañías de seguros o proveedores.

g) Seleccionar los objetivos de control y los controles para el tratamiento de riesgos

Los objetivos de control y los controles deben seleccionarse e implementarse para cumplir los requisitos identificados en la evaluación de riesgos y en el proceso de tratamiento de riesgos.

h) Obtener la aprobación por parte de la Dirección de los riesgos residuales propuestos.

Los controles propuestos en la Norma en el anexo A, deben seleccionarse a medida que sirvan para satisfacer los requisitos identificados. Estos controles pueden ser complementados por controles adicionales.

Cada uno de estos literales debe contener las consideraciones necesarias para evaluar los riesgos de los dispositivos móviles a ser utilizados para prestar el servicio o con mayor relevancia analizar los dispositivos móviles de sus empleados que llevan su propio dispositivo (BYOD).

- **ITIL**

La buena práctica ITIL, en su definición de estrategia de servicio no describe una etapa de análisis de riesgos que afecten la seguridad de la información, sino que se enfoca en los riesgos de una inadecuada estrategia de diseño de servicio.

d) Identificar controles externos implementados en los dispositivos móviles.

Debe tomarse en cuenta que no todos los controles a implementar son responsabilidad de la compañía, ya que estos equipos ya contienen controles predeterminados por los fabricantes a nivel de hardware, sistema operativo y a nivel de aplicación.

Muchos *firmware,* han sido desarrollados para proteger de forma combinada al dispositivo por un contrato de hardware y servicios móviles. Algunos dispositivos están equipados con circuitos estandarizados para propósitos de seguridad. En resumen, los controles de la capa de hardware y firmware existentes proporcionan un grado de seguridad que es bastante fácil de usar.

A nivel operativo, los proveedores han optado por una variedad de modelos de seguridad subyacentes con diferentes niveles de transparencia al usuario o administradores de seguridad. Estos pueden ser utilizados para implementar políticas de seguridad específicas del dispositivo o las políticas de configuración. En el lado del proveedor, construye sistemas operativos personalizados (en los dispositivos de marca) son la regla y no la excepción. Estos permiten a los controles de seguridad del proveedor impulsada, incluyendo a distancia parches y, de forma limitada, el mando a distancia y control.

La capa de control secundario permite a las empresas implementar herramientas especializadas y soluciones como el cifrado de terceros, encapsulación o firmware personalizado construido para la empresa. Si bien la posibilidad de utilizar este tipo de herramientas puede ser tentadora, también plantea cuestiones de apoyo a un gran número de usuarios y dispositivos móviles.

Controles provistos son: Protección contra Malware, Administración de seguridad de la red y conectividad, Administración de “Endpoint” o controles pre-aplicados para mantener la integridad del sistema del dispositivo, Administración de identidad de usuario y acceso lógico.

e) Identificar controles a nivel operativo.

La gestión de seguridad de los dispositivos móviles involucra principios de seguridad, normas y buenas prácticas.

Para poder implementar los controles requeridos para mitigar los riesgos identificados, es necesario inicialmente definir políticas las cuales posteriormente van a ser operativizadas en la ejecución de los controles en los procesos.

Cuando se aplica a la seguridad de los dispositivos móviles, la empresa debe tener en cuenta cómo se utilizan los dispositivos móviles y lo que hace sentido en términos de describir y formalizar la seguridad.

Previo a identificar estos controles se debe identificar el tipo de escenario que presenta la compañía: Dispositivos móviles centralizados, propiedad de la compañía, el número de políticas y procedimientos es más limitado, ya que existe mayor control.

En un escenario de BYOD "puro", es probable que los principios, políticas y marcos tengan que ser mucho más elaborados, ya que deberán influenciar el comportamiento de los usuarios y la seguridad.

Cobit 5 y la Norma ISO27000, establecen que para iniciar un marco de seguridad de la información se debe establecer una política de seguridad, y de acuerdo a CSX se deben considera los siguientes aspectos en su contenido:

- Analizar los procesos de negocio con dispositivos móviles, dependencias y priorizar.

- Realizar análisis de los stakeholders (internos y externos) y sus necesidades para los dispositivos móviles.
- Identificar las leyes, reglamentos y normas de gobierno para el uso de dispositivos móviles, y definir los requisitos.
- Establecer indicadores clave de rendimiento de dispositivos móviles y de informes periódicos.
- Identificar las amenazas a dispositivos móviles (en todos los niveles), anticipar las amenazas futuras a través de la tecnología, la innovación, y recopilar la evidencia sobre los incidentes e infracciones.
- Establecer un proceso de mejora continua para
- seguridad de dispositivos móviles, e incluir escenarios BYOD.
- Mantener una categorización de riesgo en un mapa de calor de los dispositivos móviles
- Establecer una clasificación de la información que reside o fluye a través de los dispositivos móviles. Incluir servicios de almacenamiento en la nube. Alinear la identidad del dispositivo móvil y acceso con la identidad corporativa.
- Desarrollar regularmente pruebas de BIA (describir bia) en los dispositivos móviles como activos relevantes en los procesos financieros o no financieros.
- Establecer un control de ciclo de vida para los dispositivos móviles, e incluir el escenario BYOD (remover o
- Aplicar gobernanza a las políticas, estándares y procedimientos operativos claves de dispositivos móviles.
- Educar a los usuarios finales en la seguridad de uso de los dispositivos móviles particularmente en el escenario BYOD.

- **COBIT 5**

A continuación mostramos los procesos habilitadores de Cobit 5 que muestran en general las actividades de control que pueden incluirse en los procedimientos existentes para la preservación de la Integridad, Confidencialidad y Disponibilidad de la información contenida en los dispositivos móviles.

APO01.03 Mantener los elementos catalizadores del sistema de gestión.
Mantener los elementos catalizadores del sistema de gestión y del entorno de control de la TI de la empresa y garantizar que están integrados y alineados con la filosofía y el estilo operativo de gobierno y de gestión de la empresa. Estos elementos catalizadores incluyen una comunicación clara de expectativas/requisitos. El sistema de gestión debería fomentar la cooperación interdepartamental y el trabajo en equipo, promover el cumplimiento y la mejora continua y tratar las desviaciones en el proceso (incluidos los fallos). Desarrollar la conciencia y la formación de seguridad para los componentes de dispositivos móviles.

APO01.06 Definir la propiedad de la información (datos) y del sistema.
Definir y mantener las responsabilidades de la propiedad de la información (datos) y los sistemas de información. Asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y su protección de acuerdo con esta clasificación. Definir la custodia de los datos usuario/administrador; definir la clase de datos y criterios de seguridad para el dispositivo móvil.

APO01.07 Gestionar la mejora continua de los procesos.
Evaluar, planificar y ejecutar la mejora continua de procesos y su madurez para asegurar que son capaces de entregarse conforme a los objetivos de la empresa, de gobierno, de gestión y de control. Considerar las directrices de la implementación de procesos de COBIT, estándares emergentes, requerimientos de cumplimiento, oportunidades de automatización y la realimentación de los usuarios de los procesos, el equipo del proceso y otras partes interesadas. Actualizar los procesos y considerar el impacto en los catalizadores del proceso. Administrar la seguridad para aplicaciones, sistema operativo y otros factores de riesgo del dispositivo móvil; desarrollar capacitaciones a los usuarios.

APO01.08 Mantener el cumplimiento con las políticas y procedimientos.
Poner en marcha procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas y otros catalizadores del marco de referencia; hacer cumplir las consecuencias del no cumplimiento o del desempeño inadecuado. Seguir las tendencias y el rendimiento y considerarlos en el diseño futuro y la mejora del marco de control. Calendarizar pruebas de cumplimiento para los dispositivos móviles.

APO02.02 Evaluar el entorno, capacidades y rendimiento actuales.
Evaluar el rendimiento del negocio interno actual y las capacidades de TI y los servicios externos de TI para desarrollar un entendimiento de la arquitectura empresarial en relación con TI. Identificar los problemas que se están experimentando y generar recomendaciones en las áreas que pueden beneficiarse de estas mejoras. Considerar los aspectos diferenciadores y las opciones de proveedores de servicios y el impacto financiero, los costes y los beneficios potenciales de utilizar servicios externos. Desarrollar una línea base de criterios de capacidad para dispositivos móviles.

APO02.03 Definir el objetivo de las capacidades de TI.
Definir el objetivo del negocio, las capacidades de TI y los servicios de TI necesarios. Esto debería estar basado en el entendimiento del entorno empresarial y sus necesidades; la evaluación de los actuales procesos de negocio, el entorno de TI y los problemas presentados; considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes o propuestas de innovación. Definir el objetivo de las capacidades de los dispositivos móviles.

APO02.04 Realizar un análisis de diferencias.
Identificar las diferencias entre el entorno actual y el deseado y considerar la alineación de activos (las capacidades que soportan los servicios) con los resultados de negocio para optimizar la inversión y la utilización de la base de activos internos y externos.
Considerar los factores críticos de éxito que apoyan la ejecución de la estrategia. Desarrollar un estudio comparativo con respecto a los dispositivos móviles. Solventar las brechas a través del proceso de administración de cambios de dispositivos móviles.

APO03.03 Seleccionar las oportunidades y las soluciones.
Racionalizar las desviaciones entre las arquitecturas de referencia y objetivo, considerando tanto la perspectiva técnica como la del negocio y agrupándolos a ambos en paquetes de trabajo del proyecto. Integrar el proyecto con todos los programas de inversión relacionados con TI para asegurar que las iniciativas relacionadas con la arquitectura estén alineadas y que estas iniciativas sean parte del cambio general en la empresa. Hacer de ello un esfuerzo en colaboración con las partes interesadas clave de la empresa y en TI para evaluar el grado de preparación de la empresa para su transformación e identificar las oportunidades, soluciones y todas las restricciones de la implementación.

APO04.01 Crear un entorno favorable para la innovación.
Crear un entorno que sea propicio para la innovación, considerando la cultura, la gratificación, la colaboración, los foros tecnológicos y los mecanismos para promover y captar ideas de los empleados. Así mismo incluir la innovación de seguridad en dispositivos móviles en el plan general de innovación.

APO04.03 Supervisar y explorar el entorno tecnológico.
Realizar una supervisión sistemática y un escaneo del entorno externo a la empresa para identificar tecnologías emergentes que tengan el potencial de crear valor (por ejemplo, realizando la estrategia corporativa, optimizando costes, evitando la obsolescencia y catalizando de una mejor manera los procesos corporativos y de TI). Supervisar el mercado, la competencia, sectores industriales y tendencias legales y regulatorias que permitan analizar tecnologías emergentes o ideas innovadoras en el contexto empresarial. Identificar y buscar técnicas emergentes en tecnología de dispositivos móviles.

APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras.
Analizar las tecnologías emergentes identificadas y/u otras sugerencias de innovación TI. Trabajar con las partes interesadas para validar las suposiciones sobre el potencial de las nuevas tecnologías y la innovación. Verificar que la nueva tecnología y su tendencia de uso en los dispositivos móviles son relevantes con las necesidades del negocio.

APO04.05 Recomendar iniciativas apropiadas adicionales.
Evaluar y supervisar los resultados de las pruebas de concepto y, si son favorables, generar recomendaciones para más iniciativas y obtener el soporte de las partes interesadas. Entregar pruebas en concepto de innovación en dispositivos móviles.

APO04.06 Supervisar la implementación y el uso de la innovación.
Supervisar la implementación y el uso de las tecnologías emergentes durante la integración, adopción y durante todo el ciclo de vida económico para garantizar que se producen los beneficios prometidos y para identificar las lecciones aprendidas. Crear un mapa de ruta para mostrar la innovación en los dispositivos móviles.

APO05.02 Determinar la disponibilidad y las fuentes de fondos.
Determinar las fuentes potenciales de fondos, diferentes opciones de financiación y las implicaciones de las fuentes de financiación sobre las expectativas del retorno de inversión. Asegurarse que existe financiamiento para seguridad de los dispositivos móviles.

APO06.02 Priorizar la asignación de recursos.
Implementar un proceso de toma de decisiones para priorizar la asignación de recursos y definir las reglas para las inversiones discrecionales por parte de unidades de negocio individuales. Incluir el uso potencial de proveedores de servicio externos y considerar las opciones de compra, desarrollo y alquiler. Asignar una prioridad adecuada para la seguridad de los dispositivos móviles.

APO06.03 Crear y mantener presupuestos.
Preparar un presupuesto que refleje las prioridades de inversión que apoyen los objetivos estratégicos basado en la cartera de programas habilitados por TI y servicios de TI. Preparar y mantener un presupuesto para dispositivos móviles.

APO07.03 Mantener las habilidades y competencias del personal.
Definir y gestionar las habilidades y competencias necesarias del personal. Verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación y/o experiencia y verificar que estas competencias se mantienen, con programas de capacitación y certificación en su caso. Proporcionar a los empleados aprendizaje permanente y oportunidades para mantener sus conocimientos, habilidades y competencias al nivel requerido para conseguir las metas empresariales. Desarrollar un plan de capacitación en seguridad de dispositivos móviles.

APO09.02 Catalogar servicios basados en TI.
Definir y mantener uno o más catálogos de servicios para grupos de clientes objetivo relevante. Publicar y mantener los servicios TI activos en los catálogos. Incorporar los dispositivos móviles en el catálogo.

APO09.03 Definir y preparar acuerdos de servicio.
Definir y preparar los acuerdos de servicio basándose en las opciones de los catálogos de servicio. Incluir acuerdos de nivel de operaciones interno. Evaluar los niveles de servicio del proveedor del dispositivo móvil contra los de la

organización. Definir niveles operativos para los dispositivos móviles en uso.

APO09.04 Supervisar e informar de los niveles de servicio.
Supervisar los niveles de servicio, informar de las mejoras e identificar tendencias. Proporcionar información de gestión adecuada para ayudar a la gestión del rendimiento. Preparar reportes de desempeño de SLA, con la finalidad de validar el desempeño del proveedor.

APO09.05 Revisar acuerdos de servicio y contratos.
Llevar a cabo revisiones periódicas de los acuerdos de servicio y revisarlos cuando sea necesario.

APO10.04. Gestionar el riesgo en el suministro.
Identificar y gestionar los riesgos relacionados con la capacidad de los proveedores de proporcionar de manera continua una entrega del servicio segura, eficaz y eficiente, incluyendo los proveedores de dispositivos móviles.

DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes.
Identificar, registrar y clasificar peticiones de servicio e incidentes, y asignar una prioridad según la criticidad del negocio y los acuerdos de servicio. Definir requerimientos de incidentes de dispositivos móviles, establecer una administración de requerimientos.

DSS02.04 Investigar, diagnosticar y localizar incidentes.
Identificar y registrar síntomas de incidentes, determinar posibles causas y asignar recursos a su resolución. Verificar que los incidentes de dispositivos móviles estén en línea con la política de continuidad y recuperación de la compañía.

DSS02.05 Resolver y recuperarse ante incidentes.
Documentar, solicitar y probar las soluciones identificadas o temporales y ejecutar acciones de recuperación para restaurar el servicio TI relacionado.

DSS03.01 Identificar y clasificar problemas.
Definir e implementar criterios y procedimientos para informar de los problemas identificados en los dispositivos móviles, incluyendo clasificación, categorización y priorización de problemas, de acuerdo al esquema de clasificación.

DSS03.02 Investigar y diagnosticar problemas.
Investigar y diagnosticar problemas en los dispositivos móviles, utilizando expertos en las materias relevantes para valorar y analizar las causas raíz, incluyendo a los proveedores.

DSS03.03 Levantar errores conocidos.
Tan pronto como las causas raíz de los problemas se hayan identificado, crear registros de errores conocidos y una solución temporal apropiada, e identificar soluciones potenciales.

DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.
Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas y que incluya a los dispositivos móviles utilizados.

DSS04.04 Ejercitar, probar y revisar el BCP.
Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.

DSS04.07 Gestionar acuerdos de respaldo.
Mantener la disponibilidad de la información crítica del negocio. Proporcionar copia de seguridad a prueba de fallos para los datos de dispositivos móviles (en reposo y en el flujo).

Adicionalmente Cobit 5 define procesos habilitadores BIA y MEA, relacionados con Plan de Continuidad y de Monitoreo respectivamente.

- **ISO/IEC27001:2005**

La norma ISO 27001, tomada como referencia al igual que COBIT5 nos muestra los controles que pueden adaptarse al uso de dispositivos móviles, contenidos en el Anexo A del referido documento. Los que sugerimos son:

Control A5.1.1. Documento de política de seguridad de la información
La Dirección debe aprobar un documento de política de seguridad de la información, publicarlo y distribuirlo a todos los empleados y terceros identificados.

Control A.5.1.2 Revisión de la política de seguridad. La política de seguridad debe revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurarse que se mantenga su idoneidad, adecuación y eficacia.

Control A.6.1.8 Revisión independiente de la seguridad de la información. El enfoque de la organización para la gestión de la seguridad de la información y su implantación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.

Control A.6.2.3 Tratamiento de la seguridad en contratos con terceros. Los acuerdos con terceros que conlleven acceso, tratamiento, comunicación o gestión, bien de la información de la organización, de los recursos de tratamiento de información o bien la incorporación de productos y servicios a los recursos de tratamiento de la información.

En el literal A.7 Gestión de Activos, A7.1 Responsabilidad sobre los activos, cuyo objeto es conseguir y mantener una protección adecuada de los activos de la organización.

Control A.7.1.1 Inventario de activos. Todos los activos deben estar claramente identificados y debe elaborarse y mantenerse un inventario de todos los activos importantes.

Control A.7.1.2 Propiedad de los activos: Toda la información y activos asociados con los recursos para el tratamiento de la información deben tener un propietario que forme parte de la organización y haya sido designado como propietario.

Control A.7.1.3 Uso aceptable de los activos. Se deben identificar, documentar e implantar las reglas para el uso aceptable de la información y los activos asociados con los recursos para el procesado de la información.

Como observamos anteriormente Cobit 5, incluye procesos habilitadores con actividades de control como las mencionadas anteriormente y que son aplicables a los dispositivos móviles.

En relación a la clasificación de la información, existen dos controles:

Control A.7.2.1 Directrices de clasificación. La información debe ser clasificada según su valor, los requisitos legales, la sensibilidad y la criticidad para la organización.

Control A.7.2.2 Etiquetado y manipulado de la información. Se debe desarrollar e implantar un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación de la información.

Tal como lo mostramos con COBIT 5, la Norma ISO/IEC27001:2005 contiene en el Anexo A. Objetivos de control ya establecidos para los siguientes aspectos:

A.8 Seguridad ligada a los recursos humanos.

A8.1 Antes del Empleo
Objetivo: Asegurar que los empleados, los contratistas y los terceros entiendan sus responsabilidades y son adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de robo, fraude o de uso.

A8.2 Durante el empleo
Objetivo: Asegurar que todos los empleados, contratistas y terceros son consistentes de las amenazas y problemas que afectan a la seguridad de la información y de sus responsabilidades y obligaciones, y de que están preparados para cumplir la política de seguridad de la organización, en el desarrollo habitual de su trabajo y reducir el riesgo de error humano.

A8.3 Cese del empleo o cambio de puesto de trabajo
Objetivo: Asegurara que los empleados, contratistas y terceros abandonan la organización o cambian de puesto de trabajo de una manera ordenada.

A.9. Seguridad física y ambiental

A9.1 Áreas seguras
Objetivo: Prevenir los accesos físicos no autorizados, los daños y las intromisiones en las instalaciones y en la información de la organización.

A9.2. Seguridad de los equipos
Objetivo: Evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos o que puedan provocar la interrupción de las actividades de la organización.

A10. Gestión de comunicaciones y operaciones

A.10.1 Responsabilidades y procedimientos de operación
Objetivo: Asegurar el funcionamiento correcto y seguro de los recursos de procesamiento de la información.

A 10.2 Gestión de la provisión de servicios por terceros
Objetivo: Implantar y mantener el nivel de seguridad de la información en la provisión del servicio, en consonancia con los acuerdos de provisión de servicios por terceros.

A 10.3 Planificación y aceptación del sistema
Objetivo: Minimizar el riesgo de fallos de los sistemas.

A10.4 Protección contra código malicioso y descargable
Objetivo: Proteger la integridad del software y de la información.

A10.5 Copias de seguridad
Objetivo: mantener la integridad y disponibilidad de la información y de los recursos de tratamiento de la información.

A10.6 Gestión de la Seguridad de las Redes
Objetivo: Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

A10.7 Manipulación de los soportes
Objetivo: Evitar la revelación, modificación, retirada o destrucción no autorizada de los activos y la interrupción de las actividades de la organización.

A10.8 Intercambio de información
Objetivo: Mantener la seguridad de la información y del software intercambiados dentro de una organización y con un tercero.

A10.9 Servicios de Comercio Electrónico.
Objetivo: Garantizar la seguridad de los servicios de comercio electrónico y el uso de los mismos.

A10.10 Supervisión
Objetivo: Detectar las actividades de procesamiento de la información no autorizada.

A11 Control de Acceso

A11.1 Requisitos de negocio para el control de acceso
Objetivo: Controlar el acceso a la información.

A11.2 Gestión de Acceso de usuario
Objetivo: Asegurar el acceso de un usuario autorizado y prevenir el acceso no autorizado a los sistemas de información.

A11.3 Responsabilidades de usuario
Objetivo: Prevenir el acceso de usuarios no autorizados, así como evitar el que se comprometa o se produzca el robo de la información o de los recursos de procesamiento de la información.

A11.4 Control de Acceso a la red
Objetivo: Prevenir el acceso no autorizado a los servicios en red.

A11.5 Control de acceso al sistema operativo
Objetivo: Prevenir el acceso no autorizado a los sistemas operativos.

A11.6 Control de Acceso a las aplicaciones y a la información
Objetivo: Prevenir el acceso no autorizado a la información que contienen las aplicaciones.

La norma en el numeral A11.7 Ordenadores portátiles y teletrabajo, cuyo objetivo es garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y servicios de teletrabajo ha definido el siguiente control:

A.11.7.1 Ordenadores portátiles y comunicaciones móviles. Se debe implantar una política formal y se deben adoptar las medidas de seguridad adecuadas de protección contra los riesgos de la utilización de ordenadores portátiles y comunicaciones móviles.

A12. Adquisición, desarrollo y mantenimiento de los sistemas de información.

A12.1 Requisitos de seguridad de los sistemas de información
Objetivo: Garantizar que la seguridad está integrada en los sistemas de información

A12.2 Tratamiento correcto de las aplicaciones
Objetivo: Evitar errores, perdidas, modificaciones no autorizadas o usos indebidos de la información en las aplicaciones.

A12.3 Controles Criptográficos
Objetivo: Proteger la confidencialidad, la autenticidad o la integridad de la información por medios criptográficos.

A12.4 Seguridad de los archivos de sistema
Objetivo: Garantizar la seguridad de los archivos de sistema.

A12.5 Seguridad en los procesos de desarrollo y soporte
Objetivo: Mantener la seguridad del software y de la información de las aplicaciones.

A12.6 Gestión de la vulnerabilidad técnica
Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

A13. Gestión de Incidentes de seguridad de la información

A13.1 Notificación de eventos y puntos débiles de la seguridad de la información.
Objetivo: Asegurarse que los eventos y las vulnerabilidades de la seguridad de la información, asociados con los sistemas de información, se comunican de manera que sea posible emprender acciones correctivas oportunas.

A13.2 Gestión de incidentes de seguridad de la información y mejoras.
Objetivo: Garantizar que se aplica un enfoque coherente y efectivo a la gestión de los incidentes de seguridad de la información.

A.14 Gestión de la Continuidad del Negocio.

A.14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
Objetivo: Contrarrestar las interrupciones de las actividades empresariales y proteger los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación.

A.15. Cumplimiento

A.15.1 Cumplimiento de requisitos legales
Objetivo: Evitar incumplimientos de las leyes o de las obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad.

A.15.2 Cumplimiento de políticas y normas de seguridad y cumplimiento técnico
Objetivo: Asegurar que los sistemas cumplen las políticas y normas de seguridad de la organización.

A.15.3 Consideraciones sobre la auditoria de los sistemas de información
Objetivo: lograr que el proceso de auditoría de los sistemas de información alcance la máxima eficacia con las mínimas interferencias.

- **ITIL**

Por ser su naturaleza, una referencia para el diseño y prestación de servicios, no identificamos controles a nivel operativo que contribuyan a la seguridad de los dispositivos móviles.

A continuación mostramos la Guía de Análisis Forense en la telefonía celular, la cual puede ser utilizada en el caso que los controles de seguridad, sean vulnerados y exista un indicio de

delito. Recomendamos poner especial atención a la cadena de custodia ya que la preservación de la evidencia es fundamental si se requiere llevar un proceso judicial el caso investigado.

VI. PROPUESTA DE GUÍA DE ANÁLISIS FORENSE EN LA TELEFONÍA CELULAR

En el mundo actual el uso de la tecnología de los celulares nos rodea en la mayoría de los ámbitos, debido a eso las actualizaciones han ido evolucionando en grandes escalas en tan poco tiempo, el nivel de utilización ha llevado a convertirlos en una necesidad. Por medio de estos aparatos se pueden realizar múltiples funciones además de llamadas, envío de mensajes de texto (SMS), mensajes de multimedia (MMS), mensajes instantáneos (IM), navegar en internet, portar datos personales facilidad para realizar diverso tipo de procesos por medio de aplicaciones específicas.

Este masivo uso de celulares con tecnología GSM alrededor del mundo ha provocado que la delincuencia se organice y desarrolle en esta herramienta un punto de ataque para sus delitos.

Actualmente en El Salvador según información recopilada a través de entrevista realizada en la Unidad de Vida de la Fiscalía de la Sub Regional de Santa Tecla, departamento de La Libertad índica que un porcentaje considerable de las denuncias y casos de delito a personas naturales involucran información digital por medio de la telefonía móvil.

Los delitos informáticos aumentan en la medida que avanza la tecnología, las situaciones en las cuales los celulares están involucrados en escenas están presentes y siempre innovan en la forma de atacar, esto conlleva a que se deben utilizar técnicas de análisis que estén acorde con la nueva tecnología con el propósito de recopilar las evidencias claves que permitan recuperar la información digital del sistema quebrantado y así resolver casos delincuenciales.

En base a la situación antes expuesta el análisis forense aumenta su importancia y es necesario que esta se aplique a los dispositivos móviles principalmente a los teléfonos celulares.

CADENA DE CUSTODIA

Según el Art. 250. Del Código Procesal Penal - *La cadena de custodia es el conjunto de requisitos que, cuando sea procedente, deben observarse para demostrar la autenticidad de los objetos y documentos relacionados con un hecho delictivo*[27].

Definición utilizada por la SALA DE LO PENAL DE LA CORTE SUPREMA DE JUSTICIA del país.

"Es el conjunto de etapas o eslabones desarrollados en forma legítima y científica durante la investigación judicial, con el fin de: a) Evitar la alteración (y/o destrucción) de los indicios materiales al momento (o después) de su recopilación; y b) Dar garantía científica plena de que lo analizado en el laboratorio forense (o presentado en el juicio), es lo mismo recabado (o decomisado) en el propio escenario del delito (o en otro lugar relacionado con el hecho)." [28]

Etapas de la Cadena de Custodia

- Extracción o recolección de la prueba.
- Preservación y embalaje de la prueba.
- Transporte o traslado de la prueba.
- Análisis Forense de las pruebas.
- Custodia y preservación final hasta que se realice el debate

Ruptura de Cadena de Custodia.

Se da una ruptura de la cadena de custodia cuando no existe concordancia entre lo que se recolecto o incauto en el escenario del delito al procesado y lo que se ha ingresado al proceso.

Siendo el análisis forense parte de la cadena de custodia y con el propósito de contribuir a obtener en la investigación información confiable, completa y autentica se presenta la siguiente propuesta de Guía de Análisis Forense para Telefonía Móvil.

GUÍA DE ANÁLISIS FORENSE EN LA TELEFONÍA CELULAR

En esta sección se presenta una propuesta de guía metodológica para apoyar el procedimiento de análisis forense específicamente en teléfonos celulares, que llevan a cabo las instituciones encargadas de dicho proceso en nuestro país, tal es el caso de la Fiscalía General de la República (FGR) y la Policía Nacional Civil de El Salvador (PNC) .

En la Figura 4 que se muestra a continuación se definen las fases que comprenderá esta propuesta de guía.

Fig. 4. Procedimiento de análisis forense propuesto

A continuación se describen cada una de las fases presentadas en la figura anterior**.**

1. Fase preparatoria

En esta fase es necesario aislar el dispositivo e identificar el sistema, luego proceder a explorar los componentes externos que se encuentren asociados al celular como tarjetas de memoria, accesorios. Los teléfonos celulares están diseñados

para comunicarse con la red de telefonía celular y otras redes mediante networking vía bluetooth, infrarrojo o Wi-Fi la manera más recomendable de preservar los datos es aislándolos de las redes cercanas a la que pueda conectarse.

Además es necesario identificar la escena del evento, recolectar foto o video del lugar.

El personal responsable de retirar los dispositivos debe estar capacitado sobre cómo tomar posesión de un dispositivo de forma adecuada y deben tener los materiales de embalaje pertinentes para mantener un dispositivo seguro, ya que podría ser utilizado como la evidencia en un caso judicial.

Se debe tener en cuenta que algunos dispositivos pueden eliminar los datos automáticamente si ninguna examen manual el equipo puede tener herramientas instalado con el fin de mantener su información privada, este tipo de procedimientos ha aumentado en los teléfonos móviles debido a su desarrollo acelerado durante el último los últimos años.

Es importante tener en cuenta también que en la evidencia física del celular por su naturaleza puede tener las huellas de los implicados en los casos por lo cual se debe salvaguardar de hacer contacto físico tomando las debidas precauciones.

Una vez definido el estado del celular si esta encendido o apagado, se recomienda mantenerlo en el estado que se encuentra, para que no se den cambios en la memoria volátil.

Si el teléfono celular está apagado debe dejarse apagado. Si por el contrario esta encendido debe ser aislado lo más pronto posible con alguna de las opciones apropiadas.[29]

- Configurar en modo de Avión si el teléfono lo permite
- Colocarlo en una caja de Faraday
- Encender un inhibidor de señal en cercanía del teléfono
- Envolverlo con tres o más capas de papel de aluminio
- Entregar el aparato para análisis antes que se descargue la batería
- Si no se puede aislar apagar el teléfono y retirar la batería

2. Recolección de Información

En esta fase de obtención de información es necesario conocer ciertas características y elementos de los teléfonos celulares con el fin de poder planificar la estrategia de extracción de la de evidencia digital.

- Modelo, marca y sistema operativo del teléfono
- Identificar la tecnología general que utiliza el celular como por ejemplo si es GSM.
- Determinar las diversas funcionalidades de almacenamiento digital, si realiza sincronización de datos en repositorios online, si es así es recomendable aplicar más de una herramienta forense para extraer los datos del celular y de sus dispositivos de almacenamiento asociados.
- Para consultar las especificaciones técnicas y las capacidades de almacenamiento de datos de los teléfonos celulares en el caso que el aparto este encendido, se pueden realizar en los sitios www.phonescoop.com o www.mobileforensicscentral.com
- Se puede realizar la obtención de la información por medio de la adquisición física: obteniendo el volcado de la memoria tanto volátil como la no volátil. Y la adquisición lógica consiste en la extracción de toda la información, empleando las herramientas forenses apropiadas de hardware y software.
- En los diversos casos que se considere que el teléfono celular es el medio provocador del delito, se recomienda que se recopile la información sobre llamadas recibidas, realizadas, mensajes de todo tipo enviados y recibidos que se consideren un rastro para la investigación ya que esto se mantienen en la memoria volátil.
- Si se encuentra un teléfono que no tiene puerto de datos, no se tiene el cable de datos o no se existe un software o hardware forense disponible para el modelo de celular se debe dejar documentada la situación.
- En algunas ocasiones las herramientas forenses utilizadas para obtener información digital de los celulares puede tener incompatibilidades o generar reportes con información errónea, por esta razón es recomendable verificar los datos extraídos utilizando más de una herramienta forense.
- La forma de extraer los datos puede variar dependiendo de la técnica, la finalidad y profundidad con la que se requiere determinar la información en el marco de investigación judicial, algunas veces pueden necesitar algunos datos otras realizar una extracción del sistema de archivo o de la memoria física.
- Para seleccionar el tipo de software a utilizar, es importante tener en cuenta el tipo de red a la cual está conectado el teléfono y el sistema operativo. Hay diferentes tipos de software algunos especializados para los teléfonos inteligentes y otros en los dispositivos Symbian.
- Es necesario tener en cuenta que el software para análisis forense no tiene acceso directo de bajo nivel a los datos dentro de la memoria del teléfono, ya que depende de comandos basada en el sistema operativo del teléfono móvil para recuperar datos en la memoria. Por lo cual al consultar el sistema operativo, se podrían crear de cambios a la memoria del dispositivo.

3. Análisis

Fase generada por los investigadores forenses, se realiza el análisis de la información recolectada. En esta etapa de análisis se examinan los datos este proceso debe realizarse con cuidado para que no se pierdas nada de lo que pueda ser relevante para el caso.

El personal responsable de esta función debe estar capacitado en las herramientas y técnicas utilizadas para el análisis forense en teléfonos móviles. La experiencia en tales campos de especialización debe obtenerse previamente.

Es recomendable que esté relacionado con el uso de herramientas forenses y no-forenses, que este en la capacidad desconectar o unir el dispositivo y la PC o cualquier otro equipo que o programa que ayude a la extracción de la información, ya sea a través de cables o de forma inalámbrica. Si se desconoce procedimientos ciertos procedimientos técnicos se corre el riesgo de perder información o pruebas de vital importancia.

Con el fin de preservar y analizar las fuentes de evidencia digital es recomendable seguir modelos del análisis forense en los dispositivos de almacenamiento o periféricos.

Tarjeta de Memoria Externa

- Efectuar una imagen forense con la herramientas de informática forense adecuada
- Extraer la evidencia digital importante según sea requerido por el proceso judicial

Tarjeta SIM

- Crear un SIM clonado o leer la información digital de este dispositivo utilizando un lector de SIM protegido contra escritura
- En caso de tener acceso al SIM se extrae la información digital relevante
- Los tipos de información que se pueden recuperar de una tarjeta SIM incluyen la fecha, hora y números de teléfono de las llamadas realizadas desde el móvil; números de fecha y hora y el teléfono de las llamadas recibidas desde el móvil; SMS los mensajes enviados y recibidos de los datos móviles y otros, tales como detalles del libro electrónico / teléfono, fotos y videos que se han guardado en la tarjeta SIM.
- Si el SIM está bloqueado con PIN, hay que documentar y dejar constancia otra opción es utilizar el PUK si se conoce.

Al verificar los resultados obtenidos se debe considerar:

- Los datos resultantes tengan el formato apropiado según el tipo de dato asociado
- Fechas y horas sean consistentes
- Cotejar que los datos requeridos han sido extraídos verificando con los obtenidos desde el teléfono celular, utilizar más de una herramienta forense y comparar los resultados.
- Si no hay coincidencia, el examinador debe usar otra herramienta significativa para verificar la exactitud de los datos extraídos del teléfono.
- Otra alternativa para validar es por medio de valores de hash de los diferentes instrumentos del teléfono. El analista forense puede extraer el archivo del teléfono celular en un principio, y luego picadillo de los archivos extraídos.

4. Documentación y Presentación del Informe

Esta fase involucra a todo el personal que participa en el proceso, es vital asegurar la credibilidad de la información obtenida. En el informe que se genera radica la evidencia de todas las acciones, sucesos y hallazgos obtenidos durante el análisis forense. Se elabora un dictamen con el propósito de dar respuesta a los puntos de pericia informática basándose en las referencias de las evidencias digitales. Remitiendo este dictamen con los elementos probatorios siguiendo los lineamientos del proceso judicial.

El perito informático está en libertad de aplicar los conocimientos especializados de la materia, de igual manera tomar en cuenta las guías de mejores prácticas y procedimientos de estándares internacionales.

La documentación del proceso se debe llevar a cabo durante todo el tiempo en forma de notas contemporáneas relativas a lo que se hizo durante el examen. Se recomienda realizar hojas de examen en el proceso para garantizar que la información básica se registra.

Algunas notas y documentación que el analista debe incluir son:

- La fecha y hora se inició el examen
- La condición física del teléfono
- Fotos de los componentes del teléfono e individuales (por ejemplo, la tarjeta SIM y la expansión de memoria por medido de tarjeta
- El estado del teléfono cuando recibió (apagado o encendido)
- Marca, modelo, e información de identificación
- Herramientas utilizadas durante el análisis

La mayoría de las herramientas de análisis para teléfonos celulares incluyen funciones de presentación de informes, algunas veces los puntos que reportan no son suficientes para necesidades de documentación.

Se puede dar el caso que las herramientas para telefonía celular reporten información inexacta como los números ESN, MIN / MDN equivocadas, modelo, o de fecha y hora errónea de datos, por lo cual se debe tener cuidado al tomar esta información para documentar.

El proceso utilizado para extraer datos desde el teléfono, los tipos de datos extraídos y documentados y cualquier hallazgo se deben documentar con precisión en los informes. Inclusive si el analista tiene éxito en extraer los datos deseados utilizando las herramientas disponibles, la documentación adicional de la información por medio de fotografías pueden ser de utilidad, especialmente para fines de presentación judicial.

Documentos de Referencia Utilizados en Laboratorios Pericial Informáticos para pericias informáticas de teléfonos celulares [30]

- NIST (2007) Guidelines on Cell Phone Forensics, http://csrc.nist.gov/
- ACPO & 7Safe (2008) Guide for Mobile phone seizure and examination. Good Practice Guide for Computer-Based Electronic Evidence, http://7safe.com/
- SWGDE Best Practices for Mobile Phone Forensics, https://swgde.org
- Kessler, G, (2010) Cell Phone Analysis: Technology, Tools and Processes Mobile Forensics World. Chicago: Purdue Univesity.
- Murphy, C. (2010) Digital Forensics Magazine, http://digitalforensicsmagazine.com/blogs/?p=80

CLASIFICACIÓN DE HERRAMIENTAS PARA ANÁLISIS FORENSE EN TELÉFONOS CELULARES

Herramientas Utilizadas en la Fiscalía General de Republica El Salvador

- **UFED (http://www.ondata.es/recuperar/analisis-forense-moviles.htm)**

Esta es una de las herramienta informáticas forenses utilizada en las oficinas de la Fiscalía de El Salvador, UFED se aplicable en el marco del procedimiento para pericias informáticas sobre telefonía celular. Esta herramienta permite la extracción de información para una variedad de modelos telefónicos, pero como toda herramienta de informática forense tiene limitaciones y no excluye la aplicación de otras técnicas especializadas y herramientas de informática forense durante la realización de una pericia informática sobre dispositivos de telefonía celular. Este hardware tiene posibilidades de realizar extracciones lógicas y físicas. Con la primera modalidad de trabajo se puede recuperar evidencia digital desde el sistema de archivos que es administrado por el sistema operativo del dispositivo. La segunda opción permite realizar una extracción completa de información digital almacenada en la memoria del dispositivo y en la tarjeta SIM, permitiendo obtener datos eliminados y otra información digital interna del teléfono celular.

Con este dispositivo se puede desbloquear algunos modelos de teléfonos celulares que hayan sido protegidos con una contraseña, pero no tiene la capacidad de desbloquear las protecciones de la tarjeta SIM mediante el uso de PIN (Personal Identification Number). Si se da el caso se puede intentar hacer una clonación de la tarjeta SIM para acceder a la evidencia digital contenida en la memoria interna del dispositivo, pero si no es posible conocer a priori el PIN o el PUK (Personal Unlocking Key) se pierde la posibilidad de extraer la información digital del SIM.

- **I2 (http://www-3.ibm.com/software/products/es/analysts-notebook)**

Herramienta empleada en el proceso de análisis de información durante investigaciones realizadas en la Unidad de Vida de la Fiscalía General de la Republica de El Salvador, con esta herramienta se acelera la misión de investigación, análisis y seguridad con tecnología para la adquisición de datos, gestión de la información y análisis de información recibida de las telefónicas. Este software ayuda a organizaciones y comunidades globales con herramientas para combatir el crimen, fraude, terrorismo y conflictos, es utilizado en departamentos y unidades de investigación para identificar actividades delictivas dentro de sus registros y datos operativos. El software de análisis forense Analyst's Notebook de i2 es capaz de mostrar un diagrama de gente, lugares u otras entidades que muestra cómo las otras partes están vinculadas. El formato gráfico de i2 Analyst's Notebook cuenta con el estándar de facto global para compartir e intercambiar inteligencia a nivel mundial.

HERRAMIENTAS COMERCIALES PARA ANÁLISIS Y RECUPERACIÓN DE DATOS EN TELÉFONOS CELULARES

- **iPhone**

- iPhoneBrowser - Accede al sistema de archivos del iphone desde entorno gráfico. (http://code.google.com/p/iphonebrowser/)
- iPhone Analyzer- Explora la estructura de archivos interna del iphone. (http://sourceforge.net/projects/iphoneanalyzer/)
- iPhoneBackupExtractor - Extrae archivos de una copia de seguridad realizada anteriormente. (http://www.iphonebackupextractor.com/)
- iPhone Backup Browser - Extrae archivos de una copia de seguridad realizada anteriormente. (https://code.google.com/p/iphonebackupbrowser/)
- iPhone-Dataprotection - Contiene herramientas para crear un disco RAM forense, realizar fuerza bruta con contraseñas simples (4 dígitos) y descifrar copias de seguridad. (https://code.google.com/p/iphone-dataprotection/)
- iPBA2 - Accede al sistema de archivos del iphone desde entorno gráfico. (http://ipbackupanalyzer.com/)
- sPyphone- Explora la estructura de archivos interna. (https://github.com/nst/spyphone)

- **BlackBerry**

- Blackberry Desktop Manager - Software de gestión de datos y backups.

(https://swdownloads.blackberry.com/Downloads/entry.do?code=A8BAA56554F96369AB93E4F3BB068C22)

- Phoneminer- Permite extraer, visualizar y exportar los datos de los archivos de copia de seguridad. (http://www.amraksoftware.com/phoneminer/)
- Blackberry Backup Extractor - Permite extraer, visualizar y exportar los datos de los archivos de copia de seguridad. (http://www.reincubate.com/res/labs/bbbe/bbbe-latest.exe)
- MagicBerry- Puede leer, convertir y extraer la base de datos IPD. (http://menastep.com/pages/magicberry.php)

➢ **Android**

- Android-locdump. - Permite obtener la geolocalización. (https://github.com/packetlss/android-locdump)
- Androguard- Permite obtener, modificar y desensamblar formatos DEX/ ODEX/ APK/ AXML/ ARSC. (https://code.google.com/p/androguard/#Description)
- viaforensics- Framework de utilidades para el análisis forense. (https://github.com/viaforensics/android-forensics)
- Osaf- Framework de utilidades para el análisis forense. (http://www.osaf-community.org/)

➢ **XRY (http://www.msab.com)**

Aplicación de software diseñada para funcionar con el sistema operativo Windows, permite realizar una extracción forense seguro de datos entre una amplia variedad de dispositivos móviles, como teléfonos inteligentes, unidades de navegación por satélite, módems, reproductores de música y tabletas.
Diseñado y desarrollado para hacer el proceso mucho más fácil con el apoyo de miles de diferentes perfiles de dispositivos móviles y cientos de versiones de aplicaciones de teléfonos inteligentes.

➢ **Mobilyze (http://www.blackbagtech.com)**

Mobilyze es una herramienta móvil de tiraje de datos, diseñado para dar a los usuarios acceso inmediato a los datos de los dispositivos iOS y Android. Se ejecuta en cualquiera de Mac o Windows. Diseñado para la facilidad de uso, incluso para investigadores con experiencia mínima forense digitales. Sólo se conecta el smartphone o la tableta a un puerto USB en el sistema que ejecuta Mobilyze. Opciones flexibles permiten una recolección de datos completa o limitada.

➢ **SecureView2 (http://mobileforensics.susteen.com)**

Secure View proporciona datos lógicos y físicos afluentes al teléfono. Secure View tiene una base sólida para realizar y recuperar resultados avanzados, con dominio de las empresas de TI, seguridad, o situaciones delictivas. Captura contactos, historial de llamadas, mensajes de texto, MMS, Calendario Datos de programa, datos eliminados y otros datos accesibles, mientras que proporciona una interfaz gráfica de lo que es fácil de usar.

➢ **MobilEdit! (http://www.mobiledit.com)**

Permite ver, buscar o recuperar todos los datos desde un teléfono con sólo unos pocos clics. Estos datos incluyen el historial de llamadas, agenda, mensajes de texto, multimedia mensajes, archivos, calendarios, notas, recordatorios y datos de aplicación primas. También recuperar toda la información del teléfono, como IMEI, sistemas operativos, incluyendo los detalles del firmware SIM (IMSI), ICCID e información de área de ubicación. Siempre que sea posible es capaz de recuperar los datos borrados de teléfonos y eludir la contraseña, PIN y el cifrado de copia de seguridad del teléfono.

➢ **Oxygen Forensic (http://www.oxygen-forensic.com)**

Programa para computadoras diseñado para extraer la mayor cantidad posible de información de teléfonos móviles y Smartphone para propósitos de investigación. Aceptado mundial por su capacidad de: Extraer Información de dispositivos móviles. Soporta 200 modelos, permite realizar el análisis de datos exportados, garantiza la invariabilidad de los datos.

➢ **Mobile Phone Examiner (http://www.accessdata.com)**

Es una solución para investigación de dispositivos móviles autónomos que incluye capacidades mejoradas de adquisición y análisis de dispositivos inteligentes. Con un enfoque diferente a los forenses móviles digitales, MPE + permite a los examinadores forenses móviles para tomar el control de la investigación, proporcionándoles herramientas únicas necesarias para recoger rápida, fácil identificar y efectivamente obtienen los datos clave de otras soluciones pasan por alto.

➢ **DeviceSeizure (http://www.paraben.com)**

DS fue la primera herramienta forense móvil en el mercado. Diseñado desde cero para los exámenes forenses de sonido de los teléfonos celulares y otros dispositivos, DS establece el estándar del sector para las investigaciones móviles. Su herramienta debe incluir adquisiciones lógicas y

físicas, así como pasar por contraseña y el sistema de archivos extracciones en una herramienta de fácil uso.

- **Incautación Celular**

Conjunto de herramientas de software que permite a los examinadores adquirir, buscar y reportar datos asociados con los teléfonos celulares que operan sobre CDMA, TDMA, GSM y redes. Puede obtener los datos de historial de bandeja de entrada y salida de mensajes, agenda, registro de llamadas, calendario, gráficos, logos, WAP: ajustes, favoritos, SIM: GSM datos específicos.

- **BitPim**
  (http://www.bitpim.org/)

Programa de gestión de teléfono se ejecuta en Windows, Linux y Mac OS permite la visualización y manipulación de los datos del teléfono celular. Estos datos pueden ser guía telefónica, fondos de pantalla, tonos de llamada y el sistema de archivos integrados. Para obtener datos con BitPim los evaluadores deben tener el cable adecuado para conectar el teléfono y la estación de trabajo forense.

- **SIMIS (http://www.teeltech.com/mobile-device-forensic-tools/simis/)**

Permite extraer datos desde una SIM de forma segura y proteger la integridad de los hashes criptográficos. Un cable USB es necesario para operar el software en una PC de escritorio.

- **Lector de tarjetas forense**

Lector de tarjetas inteligentes con conexión USB y el software FCR dando la capacidad de adquirir datos de la tarjeta SIM sin modificaciones.

HERRAMIENTAS DE CÓDIGO ABIERTO

En la siguiente tabla se presenta un listado de herramientas de código abierto con sus respectivas características y funcionalidad, las cuales pueden servir de apoyo en el análisis forense de teléfonos móviles.

Software	Función	Características
PDA Incaution	Adquisición, exámen, informes	Soporta única interfaz de cable, teléfonos Palm OS.
Incauta celular	Adquisición, exámen, informes	Soporta recuperación interior y exterior SIM, soporta única interfaz de cable
GSM.XRY	Adquisición, exámen, informes	Soporta recuperación interior y exterior SIM, compatible con cable, interfaces bluetooh e infrarrojos
Oxigeno PM	Adquisición, exámen, informes	Ciertos teléfonos GSM, compatible con adquisición de SIM interno
Mobiledit!	Adquisición, exámen, informes	Meta ciertos modelos de teléfonos CDMA, soporta SIM interno y externo, interface de cable IR
BitPim	Adquisición, exámen	SW abierto con escritura de bloqueo, metas teléfonos GSM y CDMA que utilizan protocolos admitidos para establecer conectividad
TULP 2G	Adquisición, informes	Soporta SIM interna y externa, requiere OC tarjeta inteligente compatible con SC, lector de tarjeta SIM, soporta interfaces de cable , bluetooth e IR compatible

Tabla 5. Herramientas para Análisis Forense de Celulares

VII. CONCLUSIONES

Las empresas en El Salvador cuentan con la posibilidad de proporcionar sus servicios a través de dispositivos móviles, para lo cual deben cumplir las regulaciones existentes, por lo que se hace necesario que se utilicen las mejores prácticas internacionales como referencia para implementar controles y disminuir el riesgo de perder la integridad, confidencialidad y disponibilidad de la información de la empresa o de los clientes que accedan a través de los dispositivos móviles a los servicios ofertados.

La informática forense es una rama de la informática muy amplia e importante para poder examinar cualquier dispositivo tecnológico que pueda servir como evidencia digital en un delito, se debe tener un gran cuidado en preservar dicha evidencia ya que por ser delicada debe ser recopilada y documentada de forma confiable para que sea válida en un proceso judicial.

En un teléfono celular se puede encontrar una gran cantidad de datos e información que pertenece al propietario, lo cual puede contener varias pistas que sirvan como evidencia en un proceso legal.

Es necesario que la Unidad de Análisis de la Fiscalía subregionales de El Salvador cuente con herramientas actualizadas para el vaciado de información de datos, hacer

utilizados en el análisis forense en teléfonos celulares con el fin de identificar información para evidencias de delito y dar así repuesta a los casos y agilizar los trámites judiciales.

VIII. RECOMENDACIONES

Recomendamos a las compañías que necesiten implementar controles a nivel de gobierno corporativo y procesos operativos en el uso de dispositivos móviles que tomen como referencia las buenas prácticas establecidas por Cobit 5, la Norma ISO 27001 e ITIL, ya que cada una a través de su metodología les permitirá establecer controles de vanguardia y sumamente fuertes para mitigar los riesgos de pérdida de confidencialidad, integridad y disponibilidad de la información que se maneja a través de los diferentes dispositivos móviles.

Es importante tener en cuenta los siguientes aspectos durante el proceso de extracción de la información de teléfonos celulares: realizar procedimientos, la extracción de la información debe ser en forma lógica, llevar una estricta documentación en el registro de la cadena de custodia y seleccionar el adecuado software para el análisis forense.

IX. REFERENCIAS

Publicaciones periódicas:

[1] Diego Pinto, "Metodología de análisis forense orientada a incidentes en dispositivos móviles", Universidad de Cuenca, Volumen 5 No. especial (2014) - TIC.EC: Congreso Ecuatoriano de Tecnologías de la Información y Comunicaciones, pp. 31-41 Disponible en: http://dspace.ucuenca.edu.ec/handle/123456789/21381 (Consulta: 28 de Noviembre de 2015)

Tesis:

[2] Aguirre Linares, Oscar Carlos Ernesto & Sevillano Flores, Jorge Antonio, "Desafíos a enfrentar en la Aplicación de Leyes sobre Delitos Informáticos en El Salvador", Trabajo de Graduación para optar al Grado de Maestro en Seguridad y Gestión de Riesgos Informáticos, Universidad Don Bosco, San Salvador, El Salvador, Enero 2015.

Reportes técnicos:

[3] Tendencias de Seguridad Cibernética en Latinoamérica y el Caribe, publicado en Junio 2014.

Normas:

[4] Norma ISO/IEC27001:2005

Marcos de Referencia Internacionales:

[5] ITIL, Service Strategy, 2011

[6] ISACA, COBIT5, Procesos Catalizadores

[7] ISACA, COBIT5

Recursos en línea:

[8] Luis Ángel Gómez, "La informática forense, una herramienta para combatir la ciberdelincuencia", Disponible en: http://www.minseg.gob.ar/node/1050 (Consulta: 18 de Noviembre de 2015

[9] "Análisis Forense", Disponible en: http://www.seed-security.com/upload/pdf/Datasheet_Analsis_Forense.pdf (Consulta: 18 de Noviembre de 2015)

[10] Jeimy J. Cano, "Introducción a la informática forense" Disponible en: http://52.0.140.184/typo43/fileadmin/Revista_96/dos.pdf (Consulta: 23 de Noviembre de 2015)

[11] Julio C. Ardita, "Metodología de Análisis Forense Informático", Argentina, Buenos Aires, Disponible en: http://www.cybsec.com/upload/ADACSI_Ardita_Analisis_Forense_Informaticov2.pdf (Consulta: 25 de Noviembre de 2015)

[12] CSX CIBER security Nexus-ISACA, Securing Mobile Devices (Consulta: 10 de octubre 2015)

[13] CSX CIBER security Nexus-ISACA ,Overview of Digital Forensics. (Consulta: 10 de octubre 2015)

[14] Libertad Digital http://www.libertaddigital.com/ciencia-tecnologia/internet/2013-07-26/nuestros-moviles-una-puerta-abierta-para-el-ciberdelito-1276496148/ (Consulta 29 de noviembre 2015)

[15] Generaciones de Dispositivos Móviles https://es.wikipedia.org

[16] Sistema Global para las comunicaciones https://es.wikipedia.org/wiki/Sistema_global_para_las_comunicaciones_móviles

[17] Medios de Almacenamientos http://www.adslzone.net/2015/08/21/moviles-sin-memoria-micro-sd-como-evitar-quedarnos-sin-almacenamiento

Publicaciones sobe Análisis Forense:

[18] Revista de Información, Tecnología y Sociedad. Informática Forense para Móviles. GOMEZ OCAMPO, Lizeth Marcela. Informática Forense Para Móviles.

[En Línea]. Bogotá: [citado septiembre 20 de 2014]. Disponible en internet: <URL: http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442009000200007&script=sci_arttext (Consulta: 21 Noviembre 2015)

[19] Unificación de Evidencia Digital de Fuentes Dispares Unification of digital evidence from disparate sources (Digital Evidence Bags). Disponible en internet: <URL: http://dfrws.org/2005/proceedings/turner_evidencebags.pdf> (Consulta: 21 Noviembre 2015)

[20] Sistema Forence GSM para Telefonía Móvil YNGVAR WILLASSEN Svein. Forensics and the GSM mobile telephone system. International Journal of Digital Evidence. Disponible en internet: <URL: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0658858-BFF6-C537-7CF86A78D6DE746D.pdf> (Consulta: 21 Noviembre 2015)

[21] Proceso para el Desarrollo de Examen en Pruebas de Teléfono Celular MURPHY Cindy. Developing Process For The Examination Of Cellular Phone Evidence. Disponible en internet: <URL: http://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf (Consulta: 21 Noviembre 2015)

[22] Análisis Forense de Teléfonos Móviles CURRAN Kevin, ROBINSON Andrew, PEACOCKE Stephen, CASSIDY Sean. Mobile Phone Forensic Analysis. Disponible en internet: <URL: http://eprints.ulster.ac.uk/20680/2/IJCDF10.pdf (Consulta: 27 Noviembre 2015)

[23] Forense y Tarjetas SIM, Descripción General CASADEI Fabio, SAVOLDI Antonio, Gubian Paolo. Forensics and SIM cards: an Overview. Disponible en internet: <URL: http://www.utica.edu/academic/institutes/ecii/publications/articles/EFE3EDD5-0AD1-6086-28804D3C49D798A0.pdf (Consulta: 27 Noviembre 2015)

[24] Estudio y Análisis de Evidencia Digital en Teléfonos Celulares con Tecnología GSM para Procesos Judiciales MALEZA Jorge, SANDOVAL Karina, HIDALGO Pablo. Estudio Y Análisis De Evidencia Digital En Teléfonos Celulares Con Tecnología GSM Para Procesos Judiciales. Disponible en internet:<URL: http://bibdigital.epn.edu.ec/bitstream/15000/4903/1/Estudio%20y%20an%C3%A1lisis%20de%20evidencia.pdf (Consulta: 27 Noviembre 2015)

[25] Directrices sobre análisis forense de dispositivos móviles AYERS Rick, BROTHERS Sam y JANSEN Wayne. Guidelines on Mobile Device Forensics. NIST Special Publication 800-101 Revisión 1. Disponible en internet: URL:http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf (Consulta: 27 Noviembre 2015)

[26] Herramientas Forenses para Teléfonos Móviles AYERS Rick, JANSEN Wayne, MOENNER Ludovic, AURELIEN Delaitre. NISTIR 7250 – Cell Phone Forensic Tools: An Overview and Analysis can be accessed. Disponible en internet: <URL: http://csrc.nist.gov/publications/nistir/nistir-7250.pdf> (Consulta: 27 Noviembre 2015)

Documentos:

[27] Documento de Código Procesal Penal. Centro de Documentación Judicialhttp://www.jurisprudencia.gob.sv (Consulta: 25 Noviembre 2015)

[28] Campos Calderón, J. Federico, "La Cadena de Custodia de la Evidencia (su relevancia en el proceso penal)", Proyecto de Asistencia Técnica a los Juzgados de Instrucción y Tribunales de Sentencia, Revista Justicia de Paz Nº 10 año IV- Vol. III Sep-Dic 2001, Impreso en Talleres Gráficos UCA. Pág. 80) (Consulta: 25 Noviembre 2015)

[29] Pericias Informáticas sobre Telefonía Celular http://www.jusneuquen.gov.ar/images2/Biblioteca/ProtocoloPericiasTelefoniaCelular.pdf (Consulta: 28 Noviembre 2015)

[30] Documentos de Referencia Utilizados en Laboratorios Pericial Informáticos para pericias informáticas de teléfonos celulares. http://csrc.nist.gov/ (Consulta: 28 Noviembre 2015)

X. ANEXOS

Preguntas sobre entrevista realizada en la Fiscalía General de la República

Objetivo: Conocer el manejo y tratamiento que se le da actualmente a los dispositivos móviles cuando son utilizados como evidencia en caso de un delito y el proceso que se sigue para realizar el análisis forense a dichos dispositivos.

1. **¿La institución considera los teléfonos móviles como instrumentos de prueba para la recolección de evidencia en casos de delitos?**
   R/Si por supuesto, los dispositivos móviles son considerados evidencia, por ejemplo cuando ocurren casos de homicidio y se encuentra el teléfono celular de la víctima, eso se recolecta como evidencia, porque dentro de los dispositivos móviles podemos encontrar por ejemplo quien fue la última persona que le llamó, si es que le llamó y le dijo que se vieran en algún lugar, va a quedar plasmada la llamada o los mensajes, entonces si es evidencia.

2. **¿Se realiza en la institución análisis forense de dispositivos móviles para la búsqueda de evidencias en caso de delito?**
   R/Si se realiza el análisis forense.

3. **¿Existe en la institución una sección o unidad responsable de realizar análisis forense en dispositivos móviles?**
   R/ Si existe

4. **¿Cuál es la unidad o sección encargada para llevar a cabo el análisis forense en dispositivos móviles?**
   R/ Unidad de Análisis y Tratamiento de la Información

5. **¿Cuenta la unidad con personal especializado para realizar el análisis? ¿Cuáles son las especialidades requeridas en esa unidad?**
   R/ En la Unidad de Análisis hay personas que cuentan con conocimientos técnicos para realizar este tipo de análisis que principalmente consisten en el vaciado de información de dichos dispositivos electrónicos, pero es preferente que se haga por medio de la Policía Nacional Civil (PNC), a través de su Unidad de Informática o de Análisis que ellos tienen porque puede llegar a ver cierto conflicto en el sentido de decir, está recolectando pruebas y está produciendo pruebas el mismo ente, entonces es mejor también hacer uso de la unidad de la Policía Nacional Civil encargada de esto.
   En la FGR si hay una unidad que se encarga de eso y si hacemos uso por ejemplo de la extracción de información, pero ya a la hora de materializarlo para un proceso es mejor hacerlo a través de la Policía, porque ya hay peritos específicos que son reconocidos, en cambio en el caso de nosotros tendríamos que acreditar a estos peritos de la misma institución y existe como ese conflicto que un perito dentro de nuestra misma institución puede generar conflicto de intereses.

6. **¿Utilizan algún tipo de herramienta física y técnicas para preservar la evidencia (teléfono)?**
   R/ Si utilizamos algunas herramientas

7. **¿Cuáles son las herramientas utilizadas?**
   R/ UFED es un aparato que extrae la información del dispositivo.

8. **¿Cómo se aseguran de bloquear el contacto de los teléfonos con el exterior?**
   R/ Con eso tenemos un problema y es que la recolección de la evidencia está más que todo a cargo del técnico de la Policía Nacional Civil, uno es el encargado de dirigir la escena, de decir esta evidencia se recolecta, esta no, entonces el problema es que a veces el técnico no apaga el teléfono, simplemente lo envuelve, lo sella, lo rotula, pero el teléfono queda en uso, recibiendo mensajes, llamadas, lo cual tampoco implica mayor problema porque nosotros tenemos la hora exacta en que se incautó este dispositivo y también podemos darnos cuenta que solo son llamadas y mensajes entrantes.

9. **¿Cuentan con un laboratorio para realizar el análisis forense en los teléfonos celulares?**
   R/si en la Unidad de Análisis

10. **¿Cuál es el tipo de información más común que recolectan en el proceso de análisis forense en teléfonos celulares?**
    R/ Se recolecta información tal como: bitácora de llamadas, hora y fecha de mensajes de texto y llamadas.

11. **¿Utilizan herramientas informáticas en los análisis forenses? ¿Cuáles herramienta utilizan?**
    R/ Se utiliza UFED, el cual sirve para extraer la información del dispositivo. También se utiliza un programa llamado I2 para ordenar y clasificar la información que se ha extraído, también permite procesar la bitácora de llamadas, generar gráficos y hacer una línea de tiempo, conocer la frecuencia de llamadas. A veces no es necesario tener el teléfono, basta con tener el número del teléfono de la persona que nos interesa y con ese número de teléfono nosotros pedimos bitácoras de llamadas y este programa I2 nos ayuda a procesar estas bitácora de llamadas.

12. **¿Varían esas herramientas de acuerdo a marca y modelo de los teléfonos?**
    R/Si y en los teléfonos de último modelo o más recientes a veces no se puede vaciar la información, hay problema para realizar el vaciado, se necesita la actualización y a veces no se cuenta con ella.

13. **¿En la institución se utilizan controles de estándares internacionales para salvaguardar la seguridad de las pruebas digitales? (Si respuesta es positiva proceda a pregunta 14 sino 15)**
    R/Lo desconozco, seguramente la Unidad de Análisis maneja esa información, ellos podrían darle mayor información, porque ellos manejan la parte técnica y todo lo relacionado a los dispositivos.

14. **¿Los controles utilizados están alineados a los principales marcos de trabajo de gestión de la seguridad como COBIT, ITIL o en las buenas prácticas de las Normas ISO especificadamente las 27001? (si respuesta es negativa preguntar ¿Cuáles utilizan?)**
    R/No se tiene respuesta

15. **¿Existe en el país alguna Ley que esté relacionada con el análisis forense en telefonía móvil?**
    R/No, no hay ninguna Ley, hay un proyecto de Ley de Delitos informáticos, pero según tengo entendido está enfocada a los delitos propiamente y no tanto a la extracción de la información, nosotros lo que hacemos es que seguimos la regla de la cadena de custodia, y esta es la que nos permite asegurar que cierta información proviene de un teléfono celular, asegurando quien lo ha recolectado, que se ha hecho, nos aseguramos los pasos que ha tenido un teléfono para llegar al peritaje.

16. **¿Cuáles son los tipos de delito en el país en lo los cuales son frecuentes las pruebas de delito por teléfono móvil?**
    R/ Los homicidios, amenazas, delitos informáticos por ejemplo, cuando se reproduce la pornografía, cuando un hombre toma fotos a una mujer, el caso de las extorsiones, porque la mayoría son vías telefónicas, en ese caso se usa mucho el análisis de celulares.

17. **¿La institución trabaja con algún tipo de acuerdo con las telefónicas que operan en el país?**
    R/ Sí, pero siempre canalizado por medio de la Unidad de Análisis, nosotros hacemos la petición a la Unidad de Análisis y esta unidad se encarga de procesar toda la información. Tenemos acuerdo con todas las telefónicas,

18. **¿Colaboran las empresas telefónicas que operan en el país con los procesos de recolección de evidencias en la telefonía móvil?**
    R/ Si, ellos mandan a la bitácora de llamadas de acuerdo a la fecha solicitada, esta información contiene llamada realizada y tiempo, mensajes realizados y a que numero, el contenido del mensaje y llamada no se puede saber,