UNIVERSIDAD TECNOLÓGICA ISRAEL

CARRERA DE SISTEMAS INFORMATICOS

“Análisis de Seguridad de la información en los Dispositivos Móviles Smartphone”

Estudiante:

Digna Dayana Cárdenas Vásquez

Tutor

Ing. Paul Diestra

Quito - Ecuador

Noviembre 2012

UNIVERSIDAD TECNOLÓGICA ISRAEL

CARRERA DE SISTEMAS

INFORMATICOS

CERTIFICADO DE RESPONSABILIDAD

Yo Ing. Paul Diestra certifico que la Srta. Digna Dayana Cárdenas Vásquez con C.C. No. 0105012611 realizo la presente tesis con título de **"Análisis de Seguridad de la información en los Dispositivos Móviles Smartphone"** y que es autor intelectual del mismo, que es original, autentica y personal.

_____

Ing. Paul Diestra

UNIVERSIDAD TECNOLÓGICA ISRAEL

CARRERA DE SISTEMAS

INFORMÁTICOS

ACTA DE SESIÓN DE DERECHOS

Yo, Digna Dayana Cárdenas Vásquez, declaro conocer y aceptar la disposición de la Normativa de la Universidad Tecnológica Israel que en su parte pertinente textualmente dice: “Forma parte del patrimonio de la Universidad la propiedad intelectual de las inversiones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

Cuenca, Diciembre 4 del 2012

UNIVERSIDA TECNOLÓGICA ISRAEL

CARRERA DE SISTEMAS

INFORMATICOS

CERTIFICADO DE AUTORIA

El documento de tesis con título **"Análisis de Seguridad de la información en los Dispositivos Móviles Smartphone"** ha sido desarrollado por Digna Dayana Cárdenas Vásquez con C.C. No. 0105012611 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de esta tesis sin previa autorización.

_____

Digna Dayana Cárdenas Vásquez

UNIVERSIDAD TECNOLÓGICA ISRAEL

AUTORIZACIÓN DE EMPASTADO

Quito Noviembre 04, 2012

OFI-002-AE-UP-12

Señorita
DIGNA DAYANA CARDENAS VASQUEZ
ESTUDIANTE DE LA CARRERA DE SISTEMAS INFORMATICOS
UNIVERSIDAD TECNOLÓGICA ISRAEL

Presente.-

De mi consideración:

Una vez revisadas las modificaciones de los informes emitidos, autorizamos al estudiante DIGNA DAYANA CÁRDENAS VÁSQUEZ, alumno de la CARRERA DE SISTEMAS INFORMATICOS, proceda con la impresión y presentación del empastado para el tema de tesis ANÁLIS DE SEGURIDAD DE LA INFORMACIÓN EN LOS DISPOSITIVOS MÓVILES SMARTPHONE, para que siga con el proceso de graduación y defensa respectiva.

Cordialmente,

Ing. Miryan Almache

MIEMBRO DEL TRIBUNAL

CC. Secretaría Académica
Archivo Unidad Especial de culminación de estudios y Titulación
/mp

DEDICATORIA

A Dios por haberme dado salud y la fortaleza para poder culminar mi objetivo y permitirme llegar hasta esta instancia.

A mi Madre la Sra. Rosenda Vásquez que ha estado apoyándome con sus buenos consejos y por la motivación constante que me brindo para poder culminar mis estudios, a mi padre, mis hermanas y sobrinos,

De manera muy especial a Karina Cárdenas ya que con su apoyo y ayuda me motivaron a no desmayar y a seguir adelante.

Hay que pensar que en este momento el sacrificio y perseverancia han dado buenos resultados por lo tanto es necesario agradecer como no a la institución que nos a brindado un poco de apoyo para la realización y culminación de nuestra vida universitaria.

AGRADECIMIENTO

Un agradecimiento para la institución ya que con las bases nos han ayudado a tener la capacidad de desenvolvernos de una manera apropiada para realizar un buen trabajo de tesina.

A mis amigos un sincero agradecimiento por aquellos momentos, experiencias y situaciones vividas que me permitieron engrandecer como personas, porque de cada uno de ellos pude aprender cosas valiosas e importantes que quedaran plasmadas en mi vida.

Y a todas aquellas personas que de una u otra forma, colaboraron para la realización de esta tesina, hago extensivo mi más sincero agradecimiento.

RESUMEN

El objetivo principal de esta tesina será el "Analizar las Seguridad de la información en los Smartphone", en este documento contendrá las seguridades de la información en las empresas, los riesgos, los problemas y las políticas en el uso de estas tecnologías, podremos observar que aplicaciones nos dan más seguridad en los Smartphone, para esto se plantea una serie de propuestas de seguridad, que mantendrá la información en el almacenada segura de la mayoría de ataques existente, con la realización de este documento no pretendemos dar una guía de seguridad de los teléfonos inteligentes, lo que se pretende es exponer las falencias de las seguridad de la información dentro de las empresas, para que con esto se tome conciencia de los riegos a los que están expuestas y así tratar de corregirlos para que la información este protegida.

ABSTRACT

The main objective of this thesis is the "Analyzing Information Security in the Smartphone" in this document contain information securities in companies, risks, issues and policies in the use of these technologies, we can see that give us more security applications in Smartphone, for this raises a number of security proposals, which will keep the information stored securely in most existing attacks, with the completion of this document does not intend to give up a guide smartphones, the aim is to expose weaknesses in the security of information within companies, so that with this awareness of the risks to which they are exposed and trying to fix them so that the information is protected.

TABLA DE CONTENIDOS

2. CAPITULO I: INTRODUCCION 8

1.1. Antecedentes 9

1.2. Formulación del problema 10

1.3. Sistematización 10

1.3.1. Diagnóstico 10

1.3.1.1. Causas 10

1.3.1.2. Efectos 10

1.3.2. Pronosticó 11

1.3.3. Control del pronóstico 12

1.4. Objetivos 13

1.4.1. Objetivo General 13

1.4.2. Objetivos Específicos 13

1.5. Justificación 14

1.5.1. Justificación Teórica 14

1.5.2. Justificación Práctica 14

1.5.3. Justificación Metodológica 15

1.6. Alcance y Limitaciones 16

1.6.1. Alcance 16

1.6.2. Limitaciones 16

1.7. Estudios de Factibilidad 16

1.7.1. Factibilidad Técnica 16

1.7.2. Factibilidad Economica 20

1.7.3. Factibilidad Operativa 21

2. CAPITULO II: MARCO DE REFERENCIA 22

2.1. Marco Teorico 22

2.1.1. Teoría de la seguridad de la información 22

2.1.2. Teoría de la Información 22

2.1.3. Teoría del sistema de Información 23

2.1.4. Teoría de la tecnologia de la Información 23

2.1.5. Teoría del Comité de Seguridad de la Información 23

2.1.6. Teoría del responsable de Seguridad Informática 23

2.1.7. Teoria de las Seguridades de información en la Empresas 24

2.1.8. Teoría de la Seguridad física y lógica: 24

2.1.9. Teoría de las Política de seguridad 26

2.1.10. Teoría de la evaluación de riesgos 26

2.1.11. Teoría de la administración de riesgos 26

2.2. Marco Conceptual.- 26
2.2.1. ¿Qué es seguridad de la información? 26
2.2.2. ¿Qué es una aplicación? 28
2.2.3. ¿Qué es encriptación de datos? 28
2.2.4. Tipos de encriptación de Datos 28

2.3. Marco Legal/Espacial 29
2.3.1. Marco Legal 29
2.3.2. Marco Espacial 30

3. CAPITULO lll: ESTRATEGIA METODOLOGICA 30

3.1. Metodología de investigación 31
3.1.1. Unidad de análisis 31
3.1.2. Tipo de Investigación 31
3.1.3. Métodos 31
3.1.4. Técnicas e Instrumentos 31

4. Capítulo IV.- RESULTADOS. 33

4.1. Análisis.. 33
4.1.1. Situación actual de las Empresas en cuanto a seguridad de la información. 33
4.1.2. Hábitos de uso de los Smartphone en las Empresas. 34

4.2. Análisis de problemas y riesgos de seguridad de los Smartphone en entornos Empresariales. 46
4.2.1. Vulnerabilidades de los Smartphone en las Empresas 47
4.2.2. Ataques a Smartphone 47
4.2.3. Problemas de seguridad de la información en las Empresas 48
4.2.4. Aspectos a considerar dentro de la protección en Smartphone ... 50
4.2.5. Protección frente a robo y perdida de los Smartphone 51
4.2.6. Herramientas y servicios que deben ser protegidas en los Smartphone 53
4.2.7. Riesgos obtenidos según análisis matriz 54
4.2.8. Riesgos de seguridad en Smartphone no controlados dentro de la Empresa 55
4.2.9. Soluciones de riesgo en seguridades de información dentro de la empresa 55
4.2.10. Normas para prevención de riesgos en el uso de información dentro de las empresas. 56

4.3. Determinar políticas de seguridad empresarial en el uso de Smartphone... 58
4.3.1. Sanciones previstas por incumplimiento 58
4.3.2. Departamento de seguridad de la Información 58
4.3.3. Políticas y reglas de control de acceso 59

4.3.4. Políticas aplicables para la gestión de los recursos en la Empresa.59
4.3.5. Políticas aplicables para el personal de la Empresa en el uso de los Smartphone en las Empresas..... 60
4.3.6. Normas aplicables en cuanto al uso de información a través de los Smartphone. 61
4.3.7. Plan de Capacitación..... 62

5. CONCLUSIONES Y RECOMENDACIONES..... 64

5.1. CONCLUSIONES 64

5.2. RECOMENDACIONES 65

BIBLIOGRAFÍA 66

ANEXOS 67

LISTA DE FIGURAS

Pagina

Figura 1. Diagrama Causa- Efecto (Espina de pescado) .....…..10

Figura 2. Comparación de los Sistemas operativos…..... ...19

LISTA DE GRAFICOS

Pagina

Tabla 1. Cuadro comparativo de causa y efecto..... 11

Tabla 2. Cuadro comparativo de efecto y control…..…….13

Tabla 3. Sstemas operativos para teléfono inteligentes …..…….18

Tabla 4. Tabla de costos de software del proyecto……. ..... .20

Tabla 5. Tabla de costos del hardware del proyecto……..... .20

Tabla 6. Tabla de costos recurso humano del proyectoo…… ..... .21

LISTA DE TABLAS

Pagina

Grafico 1. Disponibilidad de Dispsoitivos Moviles…… 35

Grafico 2. Disponibilidad de Smartphone…… ..... .35

Grafico 3. Disponibilidad de Smartphone con bluetooth, conexión a Internet y WiFi…… 36

Grafico 4. Habito de uso del Bluetooth en Smartphone…… 38

Grafico 5. Personal de la Empresa que accede a su Correo Electrónico desde el Smartphone…… 38

Grafico 6. Personal de la Empres que descarga programas y aplicaciones en el Smartphone…… .....…39

Grafico 7. Medidas de seguridad utilizadas/instalación en el Smartphone……...41

Grafico 8. Incidencias de seguridad ocurridas en el uso de Smartphone……. 42

Grafico 9. Herramientas de vulnerabilidades en Smartphone …… 46

Grafico 10. Servicios, Ataques y Herramientas de los Smartphone.... 48

Grafico 11. Servicios y Amenazas de los Smartphone……..... 49

Grafico 12. Smartphone a que están expuestos…… 51

Grafico 13. Que realizan los Software de protección para Smartphone..... 52

LISTA DE ANEXOS

Pagina

Anexo 1. Base del Anteproyecto 67

Anexo 2. Encuestas realizadas.. 73

Anexo 3. Glosario de Terminos.. 75

CAPITULO I: INTRODUCCION

1. Introducción

Actualmente nos encontramos en una época en donde la información, en todas sus formas automatizadas, formalizadas, pública o reservada, es el principal activo de toda Empresa, de igual forma, la tecnología actualmente permite la circulación ilimitada atreves de las redes locales e inalámbrica, permitiendo compartir datos y realizar operaciones en forma remota. Hoy en día es difícil encontrar un negocio, empresa u organización que se encuentre al margen de la tecnología móvil y que no dependa de la información que procesa.

Si bien es cierto que estas tecnologías son muy importantes para la mayoría de las empresas, ya que les permite un mayor desarrollo, por contrapartida se tiene la aparición de riesgos que de alguna forma afectan directamente a aquello que le da valor a toda empresa, su información, los delitos móviles se han vuelto la opción de un creciente grupo de ciber-delicuentes que hacen uso de la tecnología móvil de manera inapropiada.

Es por esta razón que las Empresas han comenzado a tomar conciencia, protegiendo sus recursos de información importantes, buscado brindar una protección adecuada, asegurando la integridad, confidencialidad y disponibilidad de la información.

Las seguridades pueden verse afectadas en tres componentes: el uso indebido de los dispositivos móviles, la falta de procesos de planificación de seguridad de la información o el desconocimiento de las personas acerca de las distintas medidas de seguridad.

El análisis de los problemas y riesgos así como la determinación de políticas de seguridad de la información permitirán a las empresas poder identificar las amenazas, vulnerabilidades y ataques que atentan contra la información almacenada en los Smartphone, así trataran de mitigarlos, implementando ciertos controles capaces de brindar un nivel aceptable de seguridad.

La seguridad de la información almacenada en los Smartphone no es un juego, requiere que se le dé la importancia necesaria, estableciendo formas de control preventivo y correctivo que sean necesarias, logrando de esta manera asegurara la continuidad de la Empresa con una seguridad aceptable y controlada.

1.1. Antecedentes

En los últimos cinco años en la ciudad de Cuenca, las tecnologías móviles han revolucionado esto comenzó con los primeros teléfonos móviles multimedia y los denominados notebooks, pero no ha sido hasta la aparición de los teléfonos inteligentes (Smartphone), cuando las personas han comenzado a considerados el enorme potencial de estas tecnologías que está influyendo en todos los aspectos económicos, sociales pero sobre todo profesionales.

Trayendo consigo el desarrollo de nuevos servicios y la creación de nuevos mercados, provocando una popularización sin precedentes y una imparable demanda de aplicaciones liderada por usuarios cada vez más exigentes y que ven en las tecnologías móviles un nuevo territorio por explorar cuyo descubrimiento está revitalizando e impulsando las industria, organizaciones y empresas de la ciudad de Cuenca y el país entero.

1.2. Formulación del problema

¿Existen actualmente seguridades de la información en los dispositivos móviles (Smartphone)?

1.3. Sistematización

1.3.1. Diagnostico

Situación actual de la seguridad de la información en la Empresa, reflejada a continuación en el diagrama causa efecto (Espina de pescado).

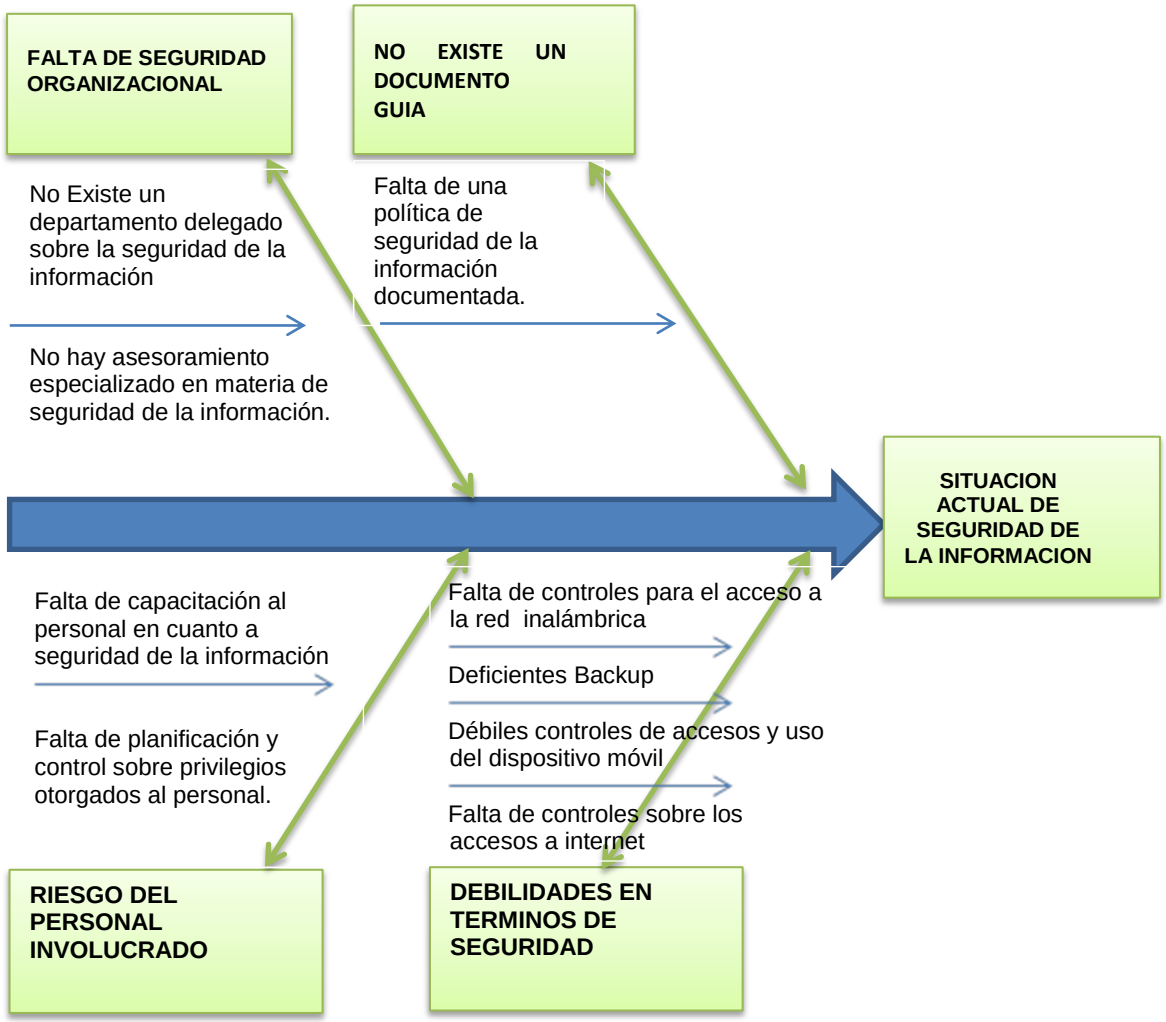


Figura 1. Diagrama Causa- Efecto (Espina de pescado)
Fuente: Dayana Cárdenas

A continuación se muestra la situación actual de seguridad de la información en la Empresa reflejada en el cuadro comparativo causa efecto.

Causa	Efecto
Falta de inducción, capacitación y sensibilización sobre riesgos.	Provocara la vulnerabilidad y ataques a la información.
Falta de definición de perfil, privilegios y restricciones del personal.	Provoca que todo el personal de la empresa tenga acceso a la información sin ninguna restricción
Fallas en permisos de usuarios (acceso a archivos).	Provocara agujeros de inseguridad
Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos).	Provoca que el personal utilice la información de la manera que la crea conveniente sin lugar a ningún tipo de sanción.
Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control.	Provoca inseguridad de la información almacenada.
Ausencia de documentación.	Provoca la no aplicación de políticas que limite el acceso a la información.

Tabla 1. Cuadro comparativo de causa y efecto

Fuente: Dayana Cárdenas

1.3.2. Pronosticó

- Con este análisis se podrá aplicar políticas que optimicen la integridad y confidencialidad de la información, garantizando la seguridad de los datos almacenados en la empresa.
- Se Pretende con este análisis reducir los riesgos de seguridad de la información de la empresa de manera que se establezca efectividad e integridad de los datos almacenados

- Otro punto que se aplicara es el de capacitar a la Empresa sobre puntos importantes: Problemática amenazas y riesgos de la seguridad de la información así como aplicar políticas reglas y normas en el uso de los teléfonos inteligentes (Smartphone)

1.3.3. Control del pronóstico

- Para controlar el avance de nuestros objetivos se realizara investigaciones claras sobre los puntos planteados en cada capítulo.
- Se realizara una recapitulación punto a punto de los temas expuestos y analizados, así tendremos un control de nuestros pronósticos y los iremos cumpliendo de manera ordenada.

A continuación se muestra la situación actual de la seguridad de la información en la empresa, reflejada en el cuadro comparativo efecto control

Efecto	Controlar
Provocara la vulnerabilidad y ataques a la información.	Se controlara la realización de capacitación acerca de las seguridades, riesgos y políticas aplicables a los teléfonos inteligentes.
Esto provoca a que todo el personal de la empresa tenga acceso a la información sin ninguna restricción	Se controlara la definición de perfiles para restringir el acceso al personal no autorizado.
Provocara agujeros de inseguridad	Se contrala si el departamento de sistemas está restringiendo el acceso a los recursos de la empresa

Provoca que el personal utilice la información de la manera que el creerá conveniente sin lugar a ningún tipo de sanción.	Se controlara que se apliquen las políticas de seguridad en base a normar y reglas internas de la empresa.
Provoca inseguridad de la información almacenada.	Se verificara que el departamento de TIC's realice los análisis de control de los datos almacenados.
Provoca la no aplicación de políticas que limite el acceso a la información.	Se controlara que los jefes y altos directivo creen un documento de políticas en base a las normas y reglas para dar a conocer al personal.

Tabla 2. Cuadro comparativo de efecto y control

Fuente: Dayana Cárdenas

1.4. Objetivos

1.4.1. Objetivo General

Analizar la seguridad de la información en las empresas a través del uso de los dispositivos móviles (Smartphone).

1.4.2. Objetivo Específico

- Analizar los problemas y riesgos de seguridad de los Smartphone en entornos empresariales.
- Determinar políticas de seguridad empresarial en el uso de Smartphone.

1.5. Justificación

1.5.1. Justificación Teórica

La información es un activo que, como otros activos importantes de la empresa, tiene valor y requiere en consecuencia una protección adecuada. La seguridad de la información protege a esta de un amplio rango de amenazas para asegurar la continuidad, minimizar los daños y maximizar el retorno de las inversiones y las oportunidades de la Empresa.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, según la Matriz para el análisis de riesgos dice: Ser un producto del proyecto de seguimiento al "Taller Centroamericano ampliando la libertad de expresión: herramientas para la colaboración, información y comunicación segura".[1]

Siendo punto clave para analizar y determinar los riesgos en el manejo de datos e información de la Empresas, la matriz se basa en una hoja de cálculo, la misma que dará resultados detallados sobre los riesgos y peligros de cada recurso (elemento de la información) de la Empresa. De tal manera el presente trabajo se basara en este control para asegurar que se cumpla los objetivos específicos de seguridad de la empresa

[1] **Gestión de riesgos en las seguridad de la información** http://protejete.wordpress.com/gdr_principal/matriz_riesgo/ copiado el 17/11/2012

1.5.2. Justificación Práctica

El principal activo o valor para toda Empresa es, sin duda, la Información, ya que cualquier problema o incidente que repercute sobre la misma va a suponer un perjuicio. Por esta razón se justifica la seguridad de la información, con el objetivo de sensibilizar a las empresas sobre la utilidad del uso de esta matriz de análisis de riesgos como ayuda para la gestión de seguridad.

Con el estudio que se realizara se tomara en cuenta todas y cada una de las problemáticas y riesgos de seguridad que nos ayudaras a tener una parametrizacion de todos los procedimiento que se pueden implementar a través de los teléfonos inteligentes.

1.5.3. Justificación Metodológica

Se optara a realizar el respectivo análisis de campo a: personal, jefes administrados, departamentales, financieros, R.R.H y altos directivos, que forme parte de la empresa para tener nuestros objetivos claros a través de un grupo meta de investigación.

Se realizara técnicas de investigación tanto en lo referente a seguridades y políticas que se utilizara para el respectivo análisis.

Se realizar un instrumento de recolección de datos (encuestas o entrevistas).

1.6. Alcance y Limitaciones

1.6.1. Alcance

- Se realizara un estudio de los teléfonos inteligentes, los cuales se utilizan para el acceso a la información concerniente al tema.
- Se realizara un plan de capacitación, así como elaboración de trípticos que contengan las seguridades, riegos y políticas aplicables para el uso de Smartphone.

1.6.2. Limitaciones

- Se llegara a solventar dudas de las seguridad de la información en si del tema propuesto
- Se tratara puntos estrictamente planteados en los objetivos específicos propuestos.
- No se realizara un sistema para demostrar las normas de seguridad.

1.7. Estudios de Factibilidad

1.7.1. Factibilidad Técnica

Dentro del enfoque de la factibilidad técnica se debe considerar tanto las variables de comparación para el desarrollo del proyecto.

Variables de comparación

a. Comparación de sistemas operativos para teléfonos inteligentes.

b. Comparación de los detalles básicos de los teléfono inteligentes

c. Aplicaciones para teléfonos inteligentes

a. Comparación de Sistemas Operativos para Teléfonos Inteligentes

Sistema Operativo	Empresa	Característica	Pst	Compatible
Android	Google	Android es un sistema operativo basado en GNU/Linux para dispositivos móviles, como teléfonos inteligentes y tablets. Fue desarrollado inicialmente por Android Inc., una firma comprada por Google en el 2005. Es el principal producto de la Open Handset Alliance, un conglomerado de fabricantes y desarrolladores de hardware, software y operadores de servicio.	1	Teléfonos Inteligentes y Tablet
iOS	Apple	Es un sistema operativo móvil de Apple desarrollado originalmente para el iPhone, siendo después usado en el iPod Touch e iPad. Es un derivado de Mac OS X, que a su vez está basado en Darwin BSD.	2	El iPhone Touch e iPad
Windows Phone 7	Microsoft	Windows Phone 7 es un sistema operativo móvil desarrollado por Microsoft, como sucesor de la plataforma Windows Mobile. Está pensado para el mercado de consumo generalista en lugar del mercado empresarial por lo que carece de muchas funcionalidades que proporciona la versión anterior. Microsoft ha decidido no hacer compatible Windows Phone 7 con	3	Samsung Ommia 7 y dispsoitivos Nokia

		Windows Mobile 6 por lo que las aplicaciones existentes no funcionan en Windows Phone 7 haciendo necesario desarrollar nuevas aplicaciones		
Symbian	Nokia y Sony Ericsson	Symbian es un sistema operativo que fue producto de la alianza de varias empresas de telefonía móvil, entre las que se encuentran Nokia, Sony Ericsson, Psion, Samsung, Siemens, Arima, Benq, Fujitsu, Lenovo, LG, Motorola, Mitsubishi Electric, Panasonic, Sharp, etc. Sus orígenes provienen de su antepasado EPOC32, utilizado en PDA's y Handhelds de PSION.	4	Nokia, Sony Ericsson, Psion, Samsung, Siemens, Arima, Benq, Fujitsu, Lenovo, LG, Motorola, Mitsubishi Electric, Panasonic, Sharp, etc
BlackBerry OS	Research in Motion	BlackBerry OS es un sistema operativo móvil desarrollado por Research in Motion para sus dispositivos BlackBerry. El sistema permite multitarea y tiene soporte para diferentes métodos de entrada adoptados por RIM para su uso en computadoras de mano, particularmente la trackwheel, trackball, touchpad y pantallas táctiles.	5	BlackBerry

Tabla 3. Sistemas operativos para teléfono inteligentes

Fuente: Dayana Cárdenas

b. Comparación de los detalles básicos de los teléfono inteligentes

Comparacion del Sistemas Operativo de los Telefono Inteligentes

	Android Cupcake	BlackBerry OS 4.7	iPhone OS 3.0	S60 5th Edition	Palm WebOS	Windows Mobile 6.5
Tipo de núcleo	Linux	Propietario	OS X	Symbian	Linux	Windows CE
Adaptabilidad	Excelente	Buena	Mala	Excelente	Excelente	Excelente
Edad de la plataforma	Joven	Madura	Adolescente	Madura	Joven	Madura
Soporte para empresas	Nada	BlackBerry	Exchange	Exchange, Domino, BlackBerry	Exchange	Exchange, Domino, BlackBerry
Tecnologías inalámbricas	GSM, WiFi	GSM, CDMA, WiFi	GSM, WiFi	GSM, WiFi	GSM, CDMA, WiFi	GSM, CDMA, WiFi

Figura 2. Comparación de los Sistemas operativos
Fuente: http://es.engadget.com/2009/03/19/la-gran-comparacion-de-los-sistemas-operativos-moviles/

c. Aplicaciones para teléfonos inteligentes

Los teléfonos inteligentes pueden personalizarse añadiendo o quitando distintas aplicaciones. Las aplicaciones son pequeños programas que añaden funcionalidades al Smartphone. Estas pueden ser desarrolladas por el fabricante del teléfono, por el responsable del sistema operativo o por un tercero.

Existen aplicaciones gratuitas que se pueden descargar del internet directamente al aparato, siendo fáciles de instalar.

1.7.2. Factibilidad Económica

a. Costo del Proyecto Software

Nombre	Costo	Total
Aplicaciones de seguridad	0.00	0.00
Herramientas de seguridad	0.00	0.00
Software de protección	40.00	60.00
Antivirus	260.00	160.00
Total Proyecto	**300.00**	**300.00**

Tabla 4. Tabla de costos de software del proyecto
Autoría: Dayana Cárdenas

b. Costo del Proyecto Hardware

Nombre	Costo	Total
PC’s	400.00	495.00
Smartphone	550.00	590.00
Router	50.00	60.00
Total Proyecto	**1000.00**	**1000.00**

Tabla 5. Tabla de costos del hardware del proyecto
Autoría: Dayana Cárdenas

c. Costo de Recursos Humano

Nombre	Costo	Total
Plan de Capacitación	200.00	200.00
Trípticos	20.00	20.00
Total Proyecto	**220.00**	**220.00**

Tabla 6. Tabla de costos recurso humano del proyecto
Autoría: Dayana Cárdenas

1.7.3. Factibilidad Operativa

La realización de este trabajo es factible ya que se cuenta con todos los materiales necesarios para la realización del análisis de seguridad, el beneficio que se obtendrá será de gran ayuda tanto dentro de la Empresa como fuera.

CAPITULO II: MARCO DE REFERENCIA

2. Marco de referencia

2.1. Marco Teórico [2]

Para el tema de estudio se van a utilizar las siguientes seguridades teóricas.

2.1.1. Teoría de la seguridad de la información

La seguridad de la información se entiendo como la preservación de las siguientes características:

a. **Confidencialidad:** Se garantice que la información sea accesible solo a aquella personas autorizadas a tener acceso a la misma
b. **Integridad:** Se salvaguarda la exactitud y totalidad de la información y los métodos de procedimiento
c. **Disponibilidad:** se garantiza que el personal autorizado tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

2.1.2. Teoría de la Información

Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

2.1.3. Teoría del sistema de Información

Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

2.1.4. Teoría tecnología de la Información

Se refiere al hardware y software operado por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Universidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.1.5. Teoría del Comité de Seguridad de la Información

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

2.1.6. Teoría del responsable de Seguridad Informática

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

2.1.7. Teoría de la seguridades de información en la Empresas

La seguridad puede entenderse como aquella regla, técnica o actividades destinadas a prevenir, proteger o resguardar lo que es considerado como susceptible de robo, perdida o daño, ya sea de manera personal o empresarial.

Es por esto que las empresas deben ejecutar normas de seguridad que haga referencia exclusivamente a la utilización de Smartphone, que cuente con el apoyo de la alta dirección y contenga entre sus objetivos:

- Brindar una referencia rápida sobre lo que implica la seguridad informática en la Empresa.
- Reducir los riesgos de error humano, las amenazas e incertidumbres en materia de seguridad en la información, estableciendo compromisos de confidencialidad con todo el personal.
- Proteger los recursos de información de la empresa.
- Dara a conocer e instruir a los integrantes de cada área informática sobre las medidas de seguridad.

2.1.8. Teoría de la Seguridad física y lógica

a. Teoría de la Seguridad Física de la información

Es muy importante ser consciente que por más que una empresa sea exigente en cuanto a seguridad de información desde el punto de vista de ataques externos,

hackers, virus, etc. La seguridad de la misma será nula si no se ha previsto como actuar frente a una perdida, robo o sustracción del teléfono inteligente.

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad así como de acceso remoto al y desde el mismo, implementados para proteger medios de almacenamientos de datos. Las principales amenazas que se prevén en la seguridad física son:

- Desastres naturales, incendios accidentales, tormentas e inundaciones.
- Amenazas ocasionadas por el hombre,
- Disturbios, sabotajes internos y externos deliberados.

b. Teoría de la seguridad Lógica de la información

Luego de ver como la información de la empresa puede verse afectada por la falta de seguridad física. Es muy importante recalcar que la mayoría de los daños no serán sobre los medios físicos sino contra la información almacenada y procesada. Es decir la seguridad lógica consiste en “la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo”.

[2] **De gerencia.com** http://www.degerencia.com/tema/tecnologia_de_informacion Copiado el 17/11/2012.

2.1.9. Teoría de las Política de seguridad

El propósito de las políticas de seguridad de la información es proteger la información y los activos de datos de la Empresa. Las políticas son guías para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación, redes, instalaciones de cómputo y dispositivos móviles.

2.1.10. Teoría de la evaluación de riesgos

Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

2.1.11. Teoría de la administración de riesgos

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

2.2. Marco Conceptual

2.2.1. ¿Qué es seguridad de la información? [3]

La información es un activo estratégico para las organizaciones. El nacimiento de las tecnologías de la información y las comunicaciones ha facilitado el

almacenamiento, procesado e intercambio de información; y estas tecnologías se han convertido en un instrumento esencial para que las organizaciones lleven a cabo su misión. Pero las nuevas tecnologías han introducido también nuevos riesgos y amenazas, por lo que la seguridad de la información se perfila, cada vez más, como una disciplina que ha de estar presente en cualquier organización.

Adicionalmente, deberán considerarse los conceptos de:

a. Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

b. Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

c. Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

d. No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

e. Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones disposiciones a las que está sujeto el Organismo.

f. Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

[3] **Servicio Nacional de Pesca** http://www.defensa.gob.es/politica/infraestructura/seguridad-informacion/ Copiado el 17/11/2012.

2.2.2. ¿Qué es una aplicación? [4]

Una aplicación móvil es un programa que usted puede descargar y al que puede acceder directamente desde su teléfono o desde algún otro aparato móvil – como por ejemplo una Tablet o un reproductor MP3.

2.2.3. ¿Qué es encriptación de datos? [5]

Encriptar es una manera de codificar la información para protegerla frente a terceros. Por lo tanto la encriptación informática sería la codificación la información de archivos o de un correo electrónico para que no pueda ser descifrado en caso de ser interceptado por alguien mientras esta información viaja por la red.

2.2.4. Tipos de encriptación de Datos [6]

a. Encriptación mediante claves simétricas: son las funciones más clásicas, es decir, se utiliza una determinada clave en la transformación de la información encriptada para conseguir desencriptarla, el problema reside en la necesidad de que todas las partes conozcan la clave.

b. Encriptación mediante claves asimétricas o públicas: existen también sistemas asimétricos de cifrado o de clave pública, cada usuario dispone de dos claves, una pública, que debe revelar o publicar para que los demás puedan comunicarse con él, y una privada que debe mantener en secreto.

[4] **Alerta en línea.gov** http://www.alertaenlinea.gov/articulos/s0018-aplicaciones-m%C3%B3viles-qu%C3%A9-son-y-c%C3%B3mo-funcionan copiado el: 17/11/2012

[5] **La revista informática.com** http://www.larevistainformatica.com/que-es-encriptacion-informatica.htm copiado el: 17/11/2012

[6] **Tecnoavancom** http://www.comercioelectronico.tecnoavan.com/criptologia.html copiado el: 17/11/2012

Cuando un usuario desea mandar un mensaje protegido, cifra el mensaje con la clave pública del destinatario. De esta manera, sólo el destinatario puede descifrar (con su clave secreta) el mensaje cifrado (Ni si quiera el emisor del mensaje puede descifrar el mensaje cifrado por él).

c. Encriptación mediante códigos de integridad: se utilizan funciones matemáticas que derivan de una huella digital a partir de un cierto volumen de datos (una huella tiene de 128 a 160 bits). Es teóricamente posible encontrar dos mensajes con idéntica huella digital; pero la probabilidad es ínfima. Si se manipulan los datos la huella cambia; y modificar los datos de forma tan sabia para obtener la misma huella es algo computacionalmente inabordable en un plazo razonable.

d. Encriptación mediante firma digital: Dado un mensaje, basta calcular su huella digital y cifrarla con la clave secreta del remitente para obtener simultáneamente la seguridad de que el contenido no se manipula (integridad), y de que el firmante es quien dice ser (autenticación). Las firmas digitales suelen ir asociadas a una fecha. La fecha de emisión (y posiblemente la fecha de vencimiento de validez) suelen proporcionarse en texto claro, e incorporarse al cálculo de la huella digital, para ligarlas irrenunciablemente.

2.3. Marco Legal/Espacial

2.3.1. Marco Legal [7]

Para este caso es necesario tomar en cuenta lo siguiente:

- Condición de acceso y utilización de los dispositivos móviles.
- Protección clasificada de información
- Derechos de los usuarios

- Derecho a la privacidad, intimidad y a los datos personales

Todo esto debe ser cumplido según menciona Conatel, Senatel: Titulo ley espacial de Telecomunicaciones reformadas, Supertel: Titulo Derechos de los Usuarios, Código Penal [artículos 197 y 213], 1974] Ley Orgánica de la Función Judicial [artículo 201], [1992] Ley Especial de Telecomunicaciones (Ley Nro. 184) Artículo 14, [1997] Ley de Control Constitucional, [1998] Constitución Política de la República de Ecuador [Artículo 23.8], [2000, en *vacatio legis*] Código de Procedimiento Penal [artículo 69.6 sobre los derechos del ofendido], [2001] Ley General de Instituciones del Sistema Financiero [artículos 88 a 94],Proyecto de Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos.

2.3.2. Marco Espacial

El lugar donde se va a realizar la investigación, será principalmente en las empresas Syscomp, MotorAlmor, Construvicor Cía. Ltda., Enlace Digital las mismas que están ubicadas en Cuenca/Ecuador, ya que es donde se puede obtener toda la información necesaria para llevar a cabo la investigación y obtención de requerimientos en forma satisfactoria.

[7]Conatel(http://www.conatel.gob.ec/site_conatel/index.php?option=com_content&view=article&catid=48%3Anormas-del-sector&id=96%3Aley-especial-de-telecomunicaciones-reformada&Itemid=103&showall=1) Copiado el 17/11/2012.
[7]Conatel (Http://www.supertel.gob.ec/index.php/table/derechos-de-los-usuarios/) Copiado el 17/11/2012.

3. CAPITULO III: METODOLOGIA

3.1. Metodología de investigación

3.1.1. Unidad de análisis

En el estudio de las unidades serán tratados las seguridades políticas y riesgos de los Smartphone, mediante el cual daré a conocer a las personas sobre las la importancia del mismo a nivel empresarial en la ciudad de Cuenca.

3.1.2. Tipo de Investigación

La presente investigación se la realizara enfocada a un análisis descriptivo del tema de trabajo propuesto, donde se pretende mostrar las cualidades y defectos de los Smartphone.

Documental: por lo que será tomado de (libros, revistas, científicas, links en internet) en donde basaremos nuestro estudio para poder obtener la información.

3.1.3. Métodos

Utilizaremos el método deductivo ya que nos basaremos de otras fuentes las mismas que están especificadas en el punto anterior.

3.1.4. Técnicas e Instrumentos

Dado de que existe algunas investigaciones previas sobre el tema de análisis se realizara una recopilación selectiva de lo que los expertos ya han investigado sobre las seguridad de la información en el usos de Smartphone dentro de las

empresas, las aplicaciones, los riesgos existentes en los mismos; todo esto con el fin de plantear un marco referencial que sirva de apoyo para desarrollar un modelo de seguridad de la información en el uso de Smartphone en las empresas.

4. CAPITULO IV: RESULTADOS

4.1. Análisis

4.1.1. Situación actual de las Empresas en cuanto a seguridad de la información.

Es indudable que el uso de los Smartphone pone en gran riesgo a la seguridad de la información en las empresas, por ello las mismas debería tomar medidas que le permita controlar la información manejada por cada personal de la empresa así previenen futuros incidentes.

Debido a los últimos avances tecnológicos, la inclusión en el mercado de los Smartphone crece a pasos agigantados permitiendo a las personas transportar sin límites la información de un lugar a otro de forma fácil y rápida, sin ser conscientes de los riesgos.

Actualmente en la mayoría de las empresas, el personal ha encontrado en estas tecnologías una herramienta no solo para uso personal si no laboral, que les permite dar respuestas inmediatas, así como tener un contacto permanente con proveedores, clientes, amigos y familiares. Por estos motivos es de vital importancia ver a la movilidad como un estilo de vida donde convergen la seguridad y la necesidad del usuario.

Por todo lo expuesto es necesario que las empresas de la Ciudad de Cuenca creen una tendencia empresarial donde los empleados puedan ingresar a las

empresas con sus dispositivos solo con fines laborales creando políticas de seguridad donde se pueda controlar el acceso a la red empresarial y la información manipulada por cada individuo en estos equipos. Hoy en día los ejecutivos, gerentes, administradores, personal administrativo entre otros llevan consigo y a todo lugar sus dispositivos móviles haciendo uso del mismo dentro de la empresa ya sea para cuestiones personales o laborales dando lugar a almacenar información en el mismo sin ningún tipo de limitación.

4.1.2. Hábitos de uso de los Smartphone en las Empresas.

La navegación hace poco copaba un 100% en equipo de hogar y oficina, sin embargo hoy en día los Smartphone en cuanto a navegación ha aumentado su uso por lo que las seguridades comienzas a suponer una amenaza para este tipo de dispositivos, por lo tanto se plantea la siguiente pregunta:

¿Existen actualmente seguridades de la información en los dispositivos móviles Smartphone?

A continuación se detalla y describe como afectan estas tecnologías de dispositivos móviles en los hábitos del personal en cuestiones de seguridad de la información dentro de las empresas.

a. Extensiones y presentaciones

Según encuestas realizadas al personal de las empresas en la ciudad de Cuenca, el personal dispone de Dispositivos móviles casi en su totalidad en el año 2012, con un porcentaje de uso de un 95%.

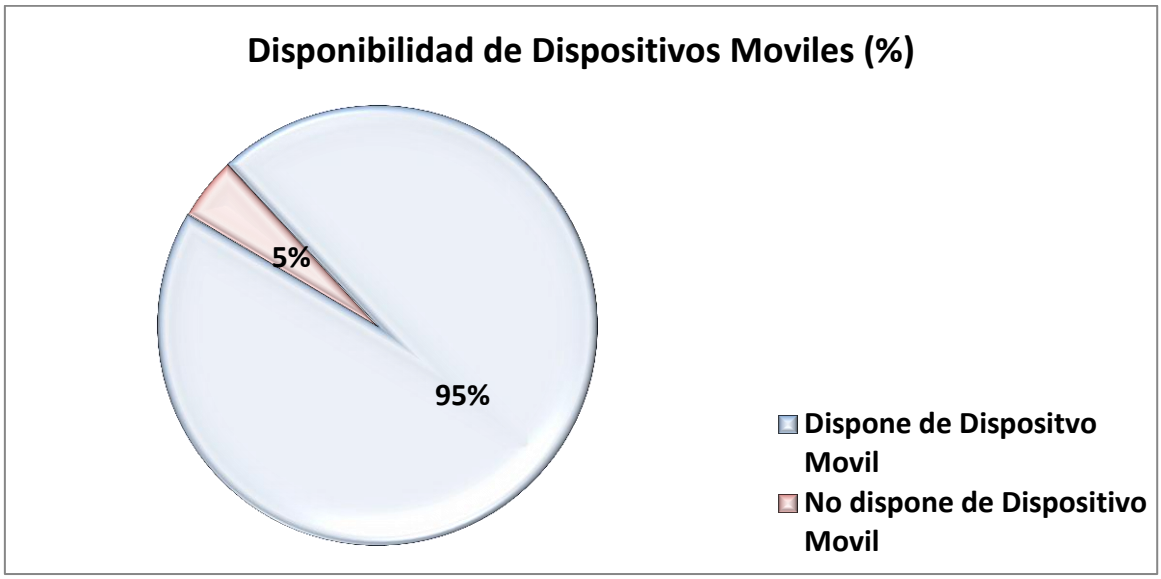


Grafico 1. Disponibilidad de Dispositivos Móviles

Fuente: Dayana Cárdenas

Desde hace algunos años atrás los Smartphone han crecido sustancialmente su popularidad, dando lugar a desplazar a los teléfonos tradicionales. Según la encuesta realizada en el presente año 2012 al personal de las empresas, el 55% de los encuestados disponen de un Smartphone.

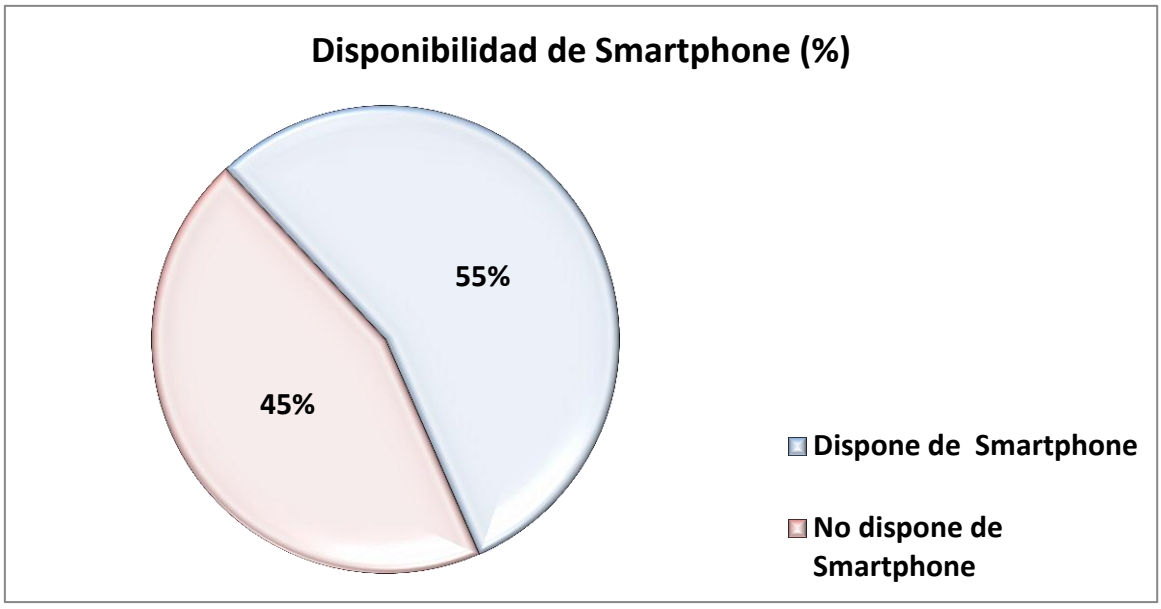


Grafico 2. Disponibilidad de Smartphone

Fuente: Dayana Cárdenas

Es importante tener en cuenta que los Smartphone tienen incorporado bluetooth y WiFi así como conexiones a internet a través de 3G/GPRS por lo que es importante analizar estos aspectos

El bluetooth es un medio de comunicación inalámbrico que nos permite el intercambio de ficheros, imágenes, videos, etc. Entre terminales cercanos e interconexiones con otros dispositivos, como radios o auriculares. La conexión 3G/GPRS como WiFi nos permiten acceder al internet, por lo tanto estas aportan mayores funcionalidades al dispositivo, permitiendo una comunicación continua en la red en casi cualquier lugar.

La presente encuesta realizada analiza si los Smartphone que poseen el personal de las empresas, se conectan ya sea al correo electrónico, redes sociales o descargas mediante este tipo de conexiones.

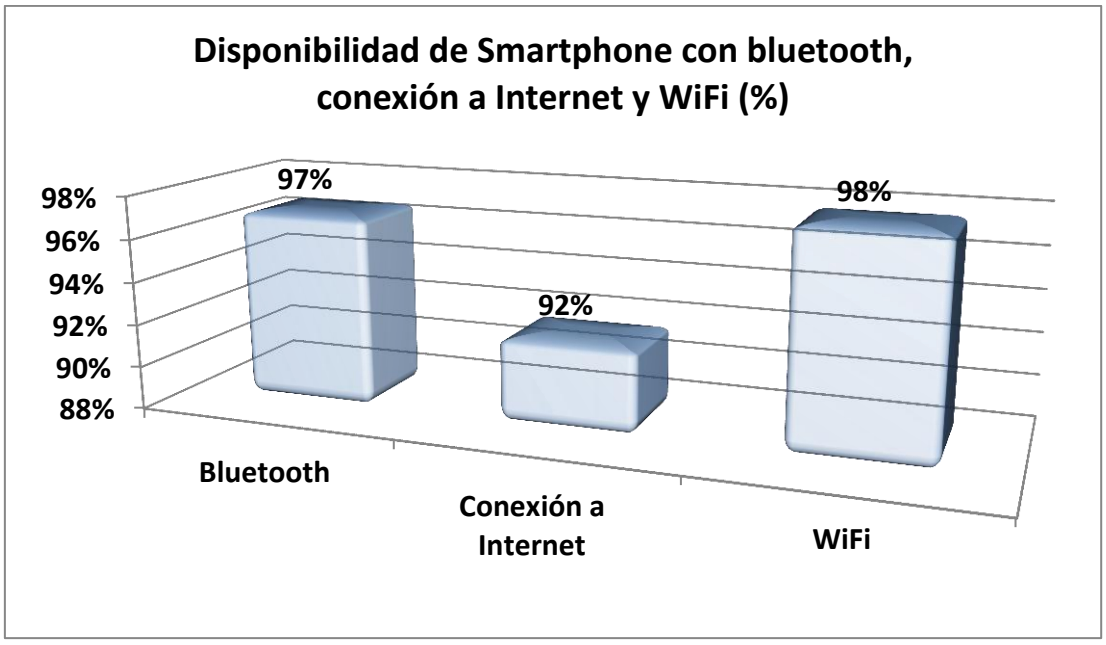


Grafico 3. Disponibilidad de Smartphone con bluetooth, conexión a Internet y WiFi
Fuente: Dayana Cárdenas

Según la encueta podemos observar que en el presente año 2012, el 97% del personal de las empresas que poseen un Smartphone disponen de bluetooth, un 92% dispone de conexión a internet mediante la tecnología 3G/GPRS, esta conexión es una característica que desde hace tiempo viene incorporada en los dispositivos móviles. En cuanto a conexiones WiFi hay un 98% que cuentan con esta ventaja.

Por lo tanto nos planteamos la siguiente pregunta:

¿Cómo utilizan los empleados estas tecnologías incorporadas en sus Smartphone?

Al analizar los hábitos del uso de Smartphone podremos ver el grado de conciencia que los empleados tienen respecto a la seguridad que se debe tener en los dispositivos en cuanto a la utilización del bluetooth.

Según las encuestas realizadas al personal de la empresa podemos apreciar que tres de cada cinco (64%) personas encienden el bluetooth cuando lo creen netamente necesario, el (16%) encontraste y como mal habito lo mantienen encendido y visible.

Es importante tener en cuenta que la ocultación de las conexión vía bluetooth cuando no se está utilizando es un buen habito de seguridad ya que evita posible intentos de conexión exterior, envíos de mensajes de correo basura o invitaciones fraudulentas, pero a más de ocultar esta conexión lo más confiable y recomendable seria el desactivarla.

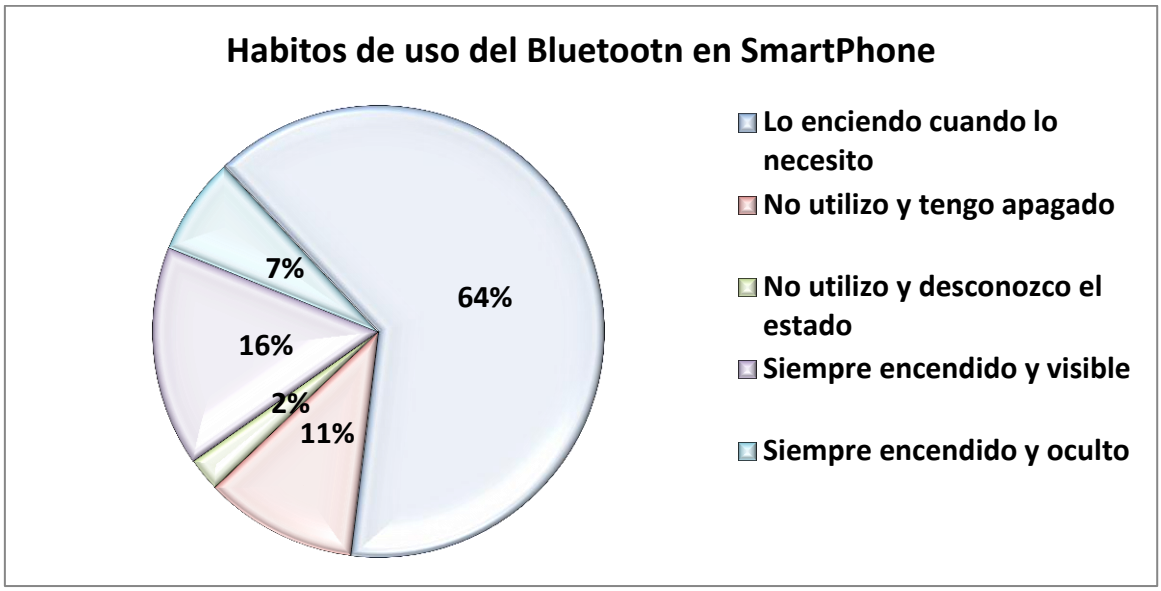


Grafico 4. Habito de uso del Bluetooth en Smartphone

Autoría: Dayana Cárdenas

A continuación se refleja en el grafico los porcentajes del personal con Smartphone que utiliza este medio para consultar su email.

Según las encuesta podemos apreciar que cuatro de cinco empleados de la empresa (64%) que disponen de Smartphone revisan los correos electrónicos desde sus teléfonos inteligentes.

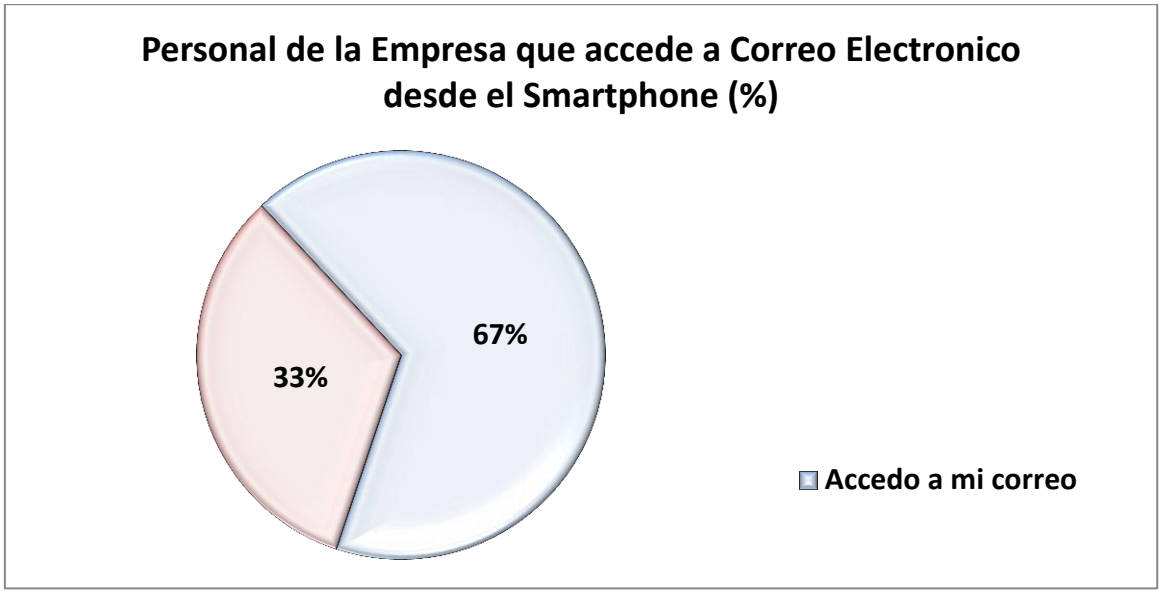


Grafico 5. Personal de la Empresa que accede a su Correo Electrónico desde el Smartphone (%)

Fuente: Dayana Cárdenas

Otra característica importante de los Smartphone es que son capaces de ejecutar programas y aplicaciones, las cuales permiten adicionar funcionalidades que necesitemos, además de que nos permiten descargar directamente de numerosos tipos de ficheros.

A continuación reflejamos en el grafico el porcentaje del personal de la empresa que se descarga programas o aplicaciones desde su Smartphone. Esto nos revela que el uso de este tipo de dispositivos por parte de los encuestados es de un 80%, reflejando un aprovechamiento al máximo de sus características. Las conexiones de WiFi también permiten la descarga de programas y aplicaciones de igual forma aprovechan esta prestación.

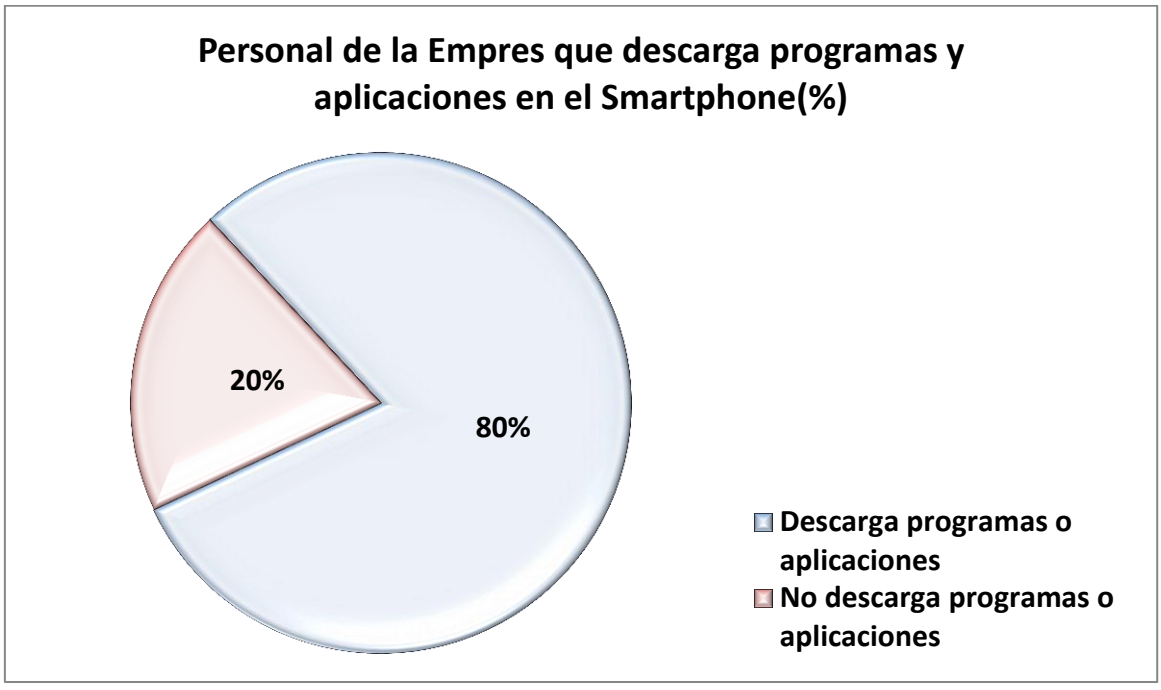


Grafico 6. Personal de la Empresa que descarga programas y aplicaciones en el Smartphone (%)
Fuente: Dayana Cárdenas

Es de vital importancia analizar en qué medida se utiliza el dispositivo para descargas de programas o aplicaciones, así como del lugar de donde provienen los ficheros, ejecutar y utilizar programas y archivos que provienen de fuentes desconocidas y dudosas pueden suponer un riesgo de seguridad.

b. Medida de seguridad utilizadas por el personal de la empresa.

A continuación se muestra el uso de diferentes medidas de seguridad que el personal de la empresa aplica para proteger sus Smartphone. En cuanto al empleo de un código PIN tenemos un (43%) que se utiliza esta medida para la protección del dispositivo, otras seguridades como realizar copias de la información y sistemas extras de contraseña (tras la inactividad) dan un porcentaje de 19%, en cuanto a contraseñas tras inactividad y protección con antivirus tenemos un 10% y 5%, también en esta encuesta se ha preguntado al personal de la empresa si tiene anotado el número de serie único del dispositivo, conocido como IMEI, un 23% afirma que realiza este buen habito de seguridad.

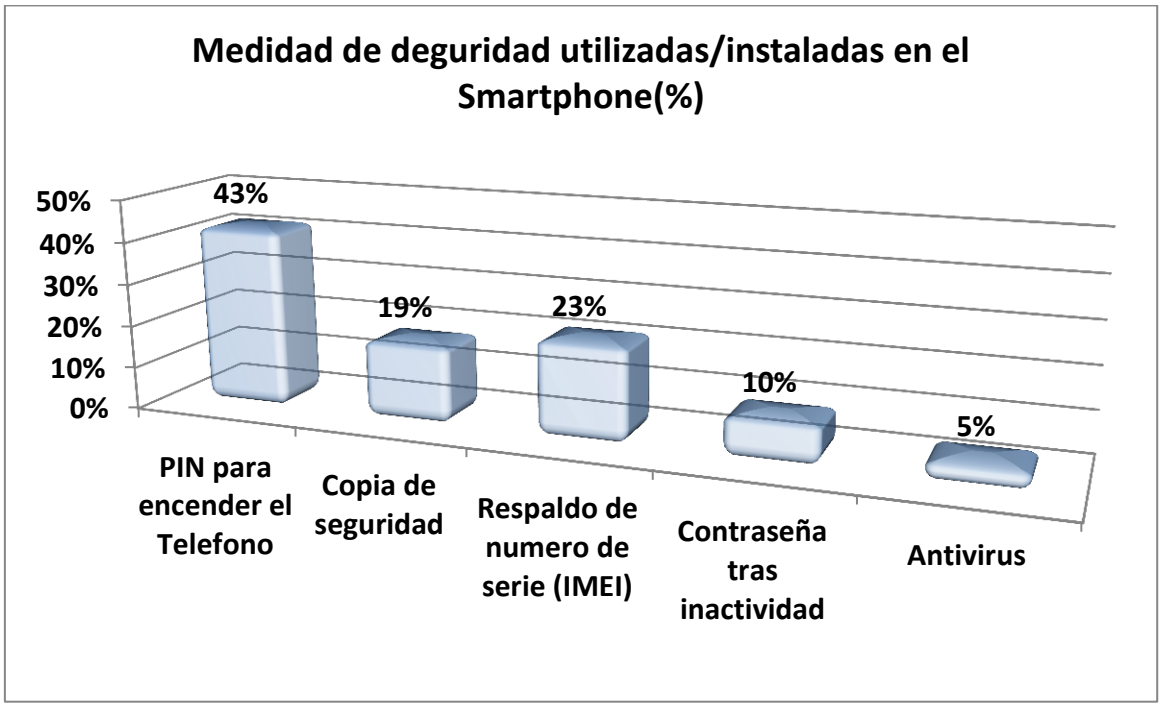


Grafico 7. Medidas de seguridad utilizadas/instalación en el Smartphone
Fuente: Dayana Cárdenas

c. Incidencias de seguridad en los Smartphone.

¿El personal de la empresa sufre incidencias de seguridad en sus Smartphone? En el Grafico podemos apreciar que un 46% declara que no ha sufrido incidencias en el uso de su Smartphone, sin embargo un 13% del personal declara haber extraviado el dispositivo y un 33% han padecido un robo del mismo, el porcentaje del personal afirma haber sufrido fraudes a través de los dispositivos móviles situándose en un 5%, en cuanto a virus y malware alcanza un porcentaje de un 3%.

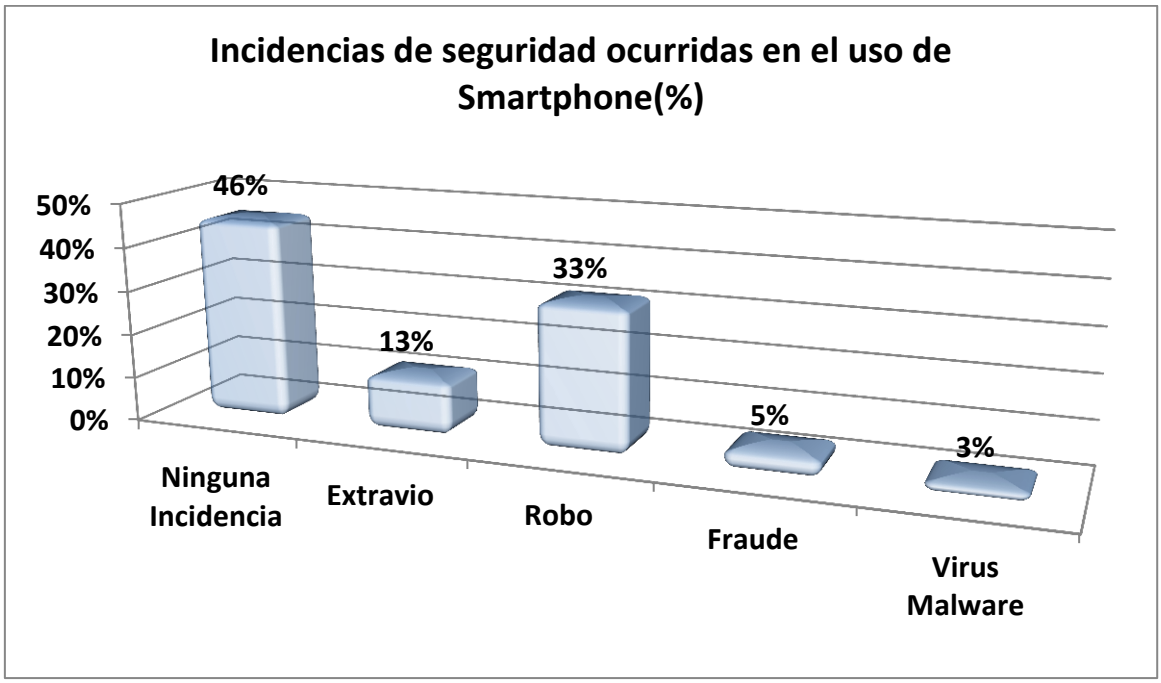


Grafico 8. Incidencias de seguridad ocurridas en el uso de Smartphone
Fuente: Dayana Cárdenas

d. Resultados de los hábitos de uso de los Smartphone en las Empresas

Los Smartphone han aumentado el uso de navegación por internet yendo en aumento, pero esto también ha producido grandes riesgos e incidencia de seguridad relacionados con los dispositivos móviles inteligentes.

Hoy en día la tecnología a evoluciona a tal punto de desplazarse del escritorio al bolsillo, la potencia de esta tecnología ha convertido a estos dispositivos móviles en instrumentos capaces de poder realizar cualquier operación que se pueda desarrollar en un ordenador personal de escritorio.

A continuación se refleja el resultado de los hábitos de uso de los Smartphone en las empresas obtenidas atreves de las encuestas realizadas diferentes empresas de la ciudad de Cuenca:

¿Cómo utilizaron los empleados estas tecnologías incorporadas en sus Smartphone?

La potente navegación y las tarifas de datos asequible en los Smartphone, provoca que las personas que poseen estos dispositivos accedan a servicios de correo, descargas de aplicaciones o utilicen Geolocalizacion. En estos tres casos el 67% hace uso del correo electrónico, el 80% realiza descargas y el 98% usa Wi-Fi para conectarse a internet.

¿Llevaron a cabo hábitos de uso seguro de Smartphone?

Los datos obtenidos mediante las encuestas demuestran que gran parte del personal de la empresa no están preparados para mitigar estas amenazas. Un 80% de los empleados descargan aplicaciones en su Smartphone desde sitios no seguros, y un 19% realiza copias de seguridad de la información almacena en el mismo.

¿El personal de la empresa sufre incidencias de seguridad en sus Smartphone?

A pesar de que el aumento de malware creado para dispositivos móviles sigue en aumento (el código malicioso para sistemas operativos móviles ha crecido), el personal de la empresa declara una incidencia muy baja de este tipo de amenazas de seguridad. Sin embargo la utilización de antivirus implantados en los teléfonos móviles es muy bajo (3%).

e. Soluciones en cuanto a los hábitos de uso de los Smartphone en las Empresas

Las soluciones que se expone a continuación pretenden servir de ayuda al personal de la empresa, así como a directivos, gerente, ejecutivos entre otros, referente a proteger y/o conservar la información almacenada en sus dispositivos móviles, así como bloquear el acceso a los mismos.

Es de vital importancia:

- Tener localizado el terminal en todo momento, para evitar el robo o acceso indebido por terceros.
- Conocer el número de IMEI que permite al personal (a través de la operadora de telefonía móvil) desactivar el terminal en caso de pérdida o robo.
- Tener activado el número PIN para que cada vez que se encienda el teléfono el acceso no sea automático.
- Realizar copias de seguridad de los contenidos de los que se disponga en el terminal y cifrar la información sensible en la memoria del teléfono.
- Activar el bloqueo automático del teléfono móvil para evitar que personas no autorizadas puedan acceder a los datos.
- En entornos empresariales en los que se maneja información altamente sensible, conectarse a servidores seguros para acceder a la información, en lugar de alojarla en el dispositivo.
- Desactivar la conexión bluetooth, Wi-Fi y 3G (siempre que sea posible esta opción) cuando no se esté usando.

- Si se realiza una conexión entre dispositivos (de móvil a móvil, o de móvil a ordenador), comprobar que ninguno de ellos se encuentre comprometido o aloje archivos infectados.
- Descargar aplicaciones desde sitios oficiales y reputados y revisar las solicitudes de permisos que aparecen. Antes de aceptar estas solicitudes, es necesario comprender y valorar a qué se está dando permiso (por ejemplo, acceso a la tarjeta de memoria, conexión a Internet, intercambio de datos, etc.).
- Vigilar el consumo y, en caso de notar incrementos bruscos en la factura, verificarlo con el proveedor de servicio telefónico móvil, ya que puede ser un indicio de fraude o de uso indebido.
- A la hora de deshacerse del terminal, realizar un borrado seguro y definitivo de la información almacenada en el mismo.

4.2. Análisis de problemas y riesgos de seguridad de los Smartphone en entornos Empresariales

4.2.1. Vulnerabilidades de los Smartphone en las Empresas

Los Smartphone almacenan gran cantidad de información sensible e identificable que un atacante podría conseguir. La preocupación es mayor cuando pensamos que los Smartphone se están introduciendo rápidamente en el entorno empresarial y podrían ser utilizados como vector de ataque comprometiendo la seguridad de la información en la empresa.

En los Smartphone se podría encontrar vulnerabilidades ampliamente conocidas como:

- Contraseñas sin codificar,
- Envió de información en texto sin ningún tipo de protección,
- Inyecciones de SQL.
- Otras vulnerabilidades que estos presentan es la capacidad que tienen de recoger información del dispositivo como lista de contactos, información del sistema operativo y hardware.

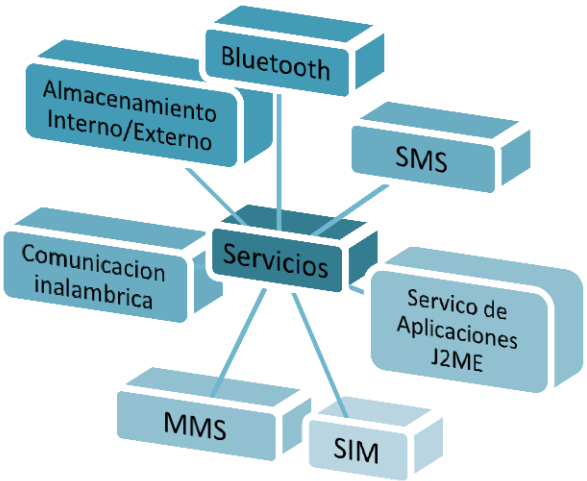


Grafico 9. Herramientas de vulnerabilidades en Smartphone
Fuente: Dayana Cárdenas

4.2.2. Ataques a Smartphone

Los ataques a dispositivos móviles inteligentes se dan principalmente por que las los directivos de las empresas no son conscientes de los riesgos al que puede estar expuesta su información en el uso de Smartphone, los mismos que han incrementado sus funciones en la red hasta asimilarse a las computadoras de escritorio o portátiles, por lo que es de esperarse que las mafias de cibercriminales los conviertan en su nuevo objetivo de sus ataques.

Las empresas ante estas amenazas tienen la exigencia de ver a estos teléfonos inteligentes como una puerta de entrada de los ataques que afectaran a la información privada que contenga la empresa.

Las nuevas funcionalidades de los Smartphone, como los sistemas de pago a través de los mismos, propician a que estos dispositivos sean cada vez más utilizados almacenando información valiosa para las mafias como datos personales y financieros de las empresas exponiéndose a fraudes.

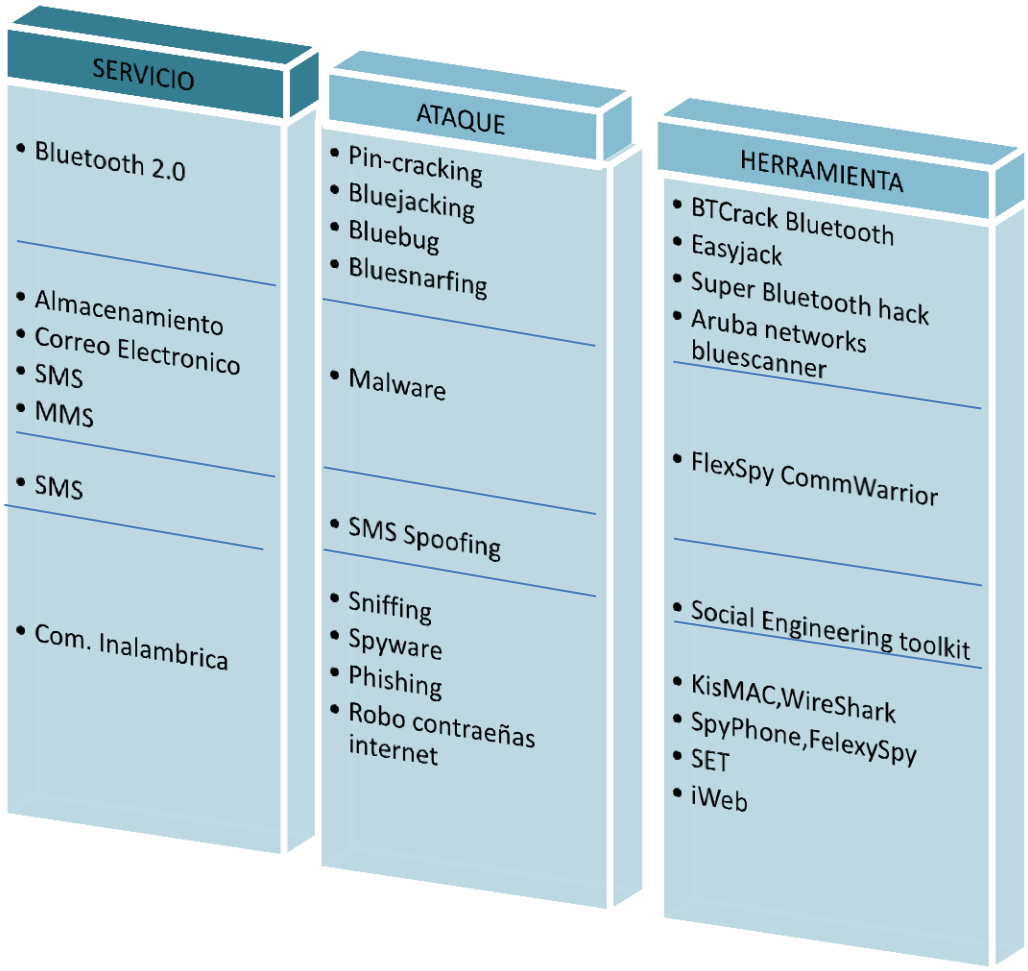


Grafico 10. Servicios, Ataques y Herramientas de los Smartphone
Fuente: Dayana Cárdenas

4.2.3. Problemas de seguridad de la información en las Empresas

¿Por qué las empresas incorporan a los teléfonos inteligentes en sus estrategias de seguridad?

Los Smartphone poseen varios usos, tanto en el entorno profesional como privado. Por lo tanto tener una protección de estas problemáticas es imprescindible. En las empresas los teléfono inteligentes son utilizados normalmente para acceder a redes de comunicación, principalmente a sistemas de telefonía y de correo electrónico, sistemas de mensajería, sistemas de gestión

y planificación de calendarios, acceso a bases de datos de contactos, por lo tanto se debe asegurar la confidencialidad de estos datos protegidos por la empresa. El ingreso al correo electrónico empresarial y la información de clientes y proveedores no se les debe permitir a terceras personas.

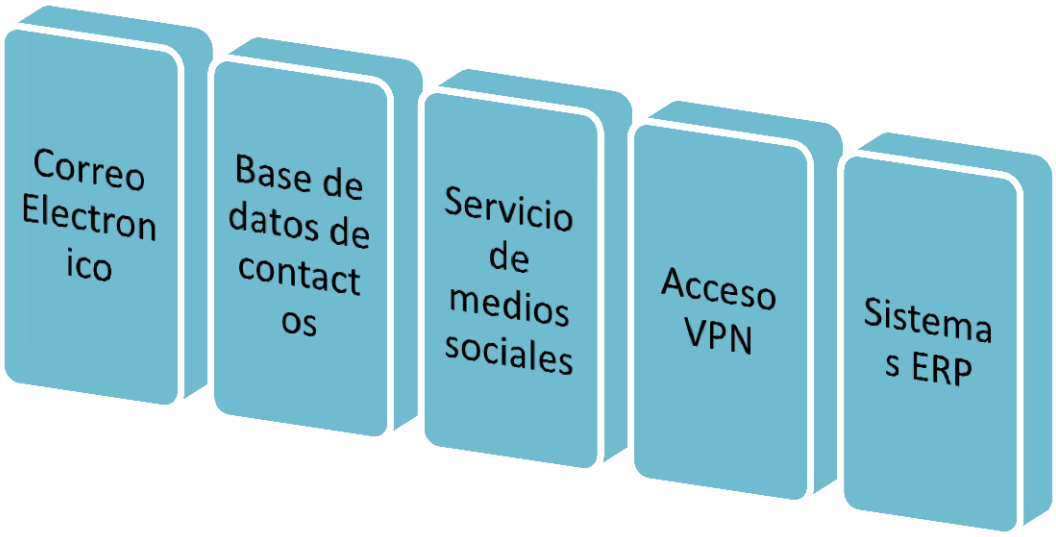


Grafico 11. Título: Servicios y amenazas de los Smartphone
Fuente: Dayana Cárdenas

Los empleados utilizan normalmente una conexión VPN para acceder a redes empresariales, mediante esta se puede acceder a archivos y aplicaciones de la empresa como los sistemas ERPs. Es muy importante que las empresas tomen acciones en estas problemáticas para evitar que el personal no autorizado acceda a información interna de la empresa, extraigan datos, o manipulen aplicaciones existentes.

Normalmente las empresas durante años han tenido implementado estrategias de protecciones que cubrían estaciones de trabajo, servidores y otros recursos de TI. Pero lamentablemente la protección de los teléfonos inteligentes todavía no está bajo esta prevención, para esto es indispensable que se cree un componente fijo

de las políticas de seguridad empresarial, así como proteger los teléfonos inteligentes de la empresa sería un paso muy acertado.

4.2.4. Aspectos a considerar dentro de la protección en Smartphone

Los Smartphone se deberían proteger en tres aspectos básicos:

a. Pérdida o Robo, según la encuesta realizada podemos observar que existe un porcentaje de 33% de personal que han perdido sus dispositivos móviles.

b. Acceso información sin autorización, existen situaciones en que otras personas obtienen acceso completo al dispositivo durante un largo periodo de tiempo, por ejemplo: el hecho de que un empleado deje su dispositivo móvil en el escritorio de su compañero y este lo tome, esto produce un riesgo real de uso no apropiado de la información empresarial mediante el acceso no autorizado.

c. Combinación de todas las demás situaciones de riesgo, malware, ataques por SMS, robo de datos mediante correos electrónicos o sitios web, los responsables de los ataques no tienen acceso físico al dispositivo.

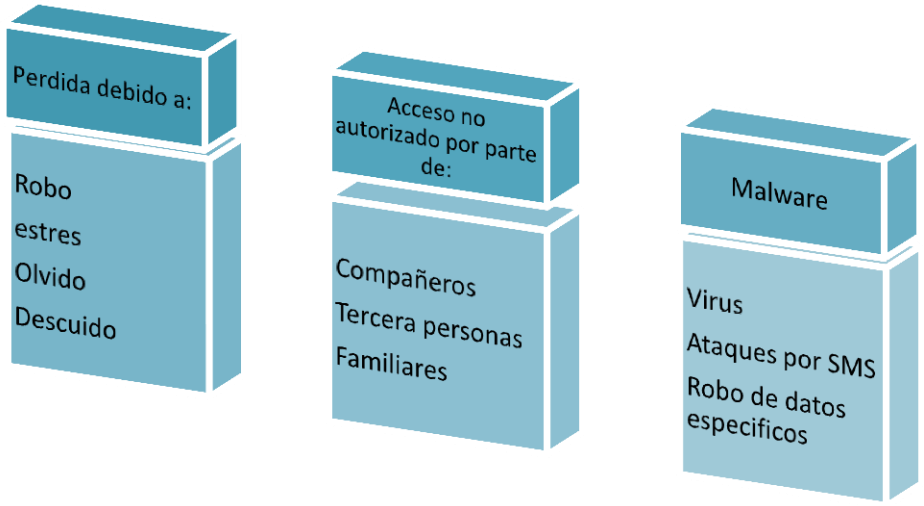


Grafico 12. Smartphone a que están expuestos
Fuente: Dayana Cárdenas

4.2.5. Protección frente a robo y perdida de los Smartphone

La pérdida o robo del Smartphone, provocaría que otra persona pueda conseguir acceso físico al dispositivo, teniendo todo el tiempo para acceder a la información almacenada en el mismo, los datos almacenados en el dispositivo no son los únicos de valor que este posee, si no también resulta de interés la información de inicio de sesión en redes empresariales o en servicios de telecomunicaciones, si hay contraseñas de servidores VPN o de correo electrónico almacenadas en el teléfono inteligente. El ladrón solo tendría que elegir la aplicación adecuada para obtener acceso a los mismos. Existe software de protección, que incluye funciones especiales de antirrobo que evitan el acceso de terceras personas a la información de los dispositivos esta sería una opción de prevención. Los teléfonos inteligentes que se extravían se los puede incluso bloquear a distancia utilizando software especiales de gestión. Los dispositivos con GPS viene implementada en

casi todos los Smartphone, esta función podría también ser utilizada para localizar al dispositivo.

Un ladrón profesional realizara medidas rápidas para evitar ser localizado por lo tanto las primera acciones que realizara el será el de retirar la tarjeta SIM. Pero en ese caso la instalación de un software que ofrezca una solución que permite localizar al dispositivo móvil aunque se haya retirado la tarjeta SIM, siendo posible enviar el número de teléfono de la tarjeta SIM insertada al legítimo dueño del teléfono.

¿Qué ocurriría si el Smartphone no puede ser bloqueado a tiempo?

En estos casos el cifrado sería una buena opción. Este es muy eficaz para proteger datos, archivos y soporte de almacenamientos, lo que asegura que solo puedan acceder a los datos aquellos que disponen de la contraseña correcta.

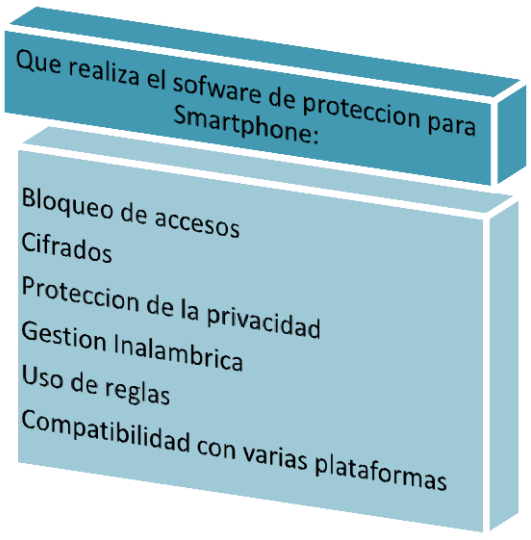


Grafico 13. Que realizan los Software de protección para Smartphone
Fuente: Dayana Cárdenas

Los Malware móvil suelen ser pasados por alto, por lo tanto se recomienda ser precavido, ya que la creciente popularidad de los Smartphone los convierte en objetivos muy importantes para los creadores de malware, lo más aconsejable seria que se tome precauciones mediante el uso de seguridad en tiempo real, es necesario realizar un análisis de malware completos, se debe contar con un módulo anti-spam. Sus funciones no deben limitarse a los mensajes de correos electrónicos sino también a mensajes de texto no deseados e incluso a llamadas.

4.2.6. Herramientas y servicios que deben ser protegidas en los Smartphone

a. App store

Es importante tener en cuenta que el único gran punto de distribución de malware de los dispositivos móviles inteligentes es la descarga de aplicaciones, sin embargo, la gran mayoría de los usuarios de Smartphone no están conscientes de la importancia de utilizar antivirus en sus dispositivos para realizar periódicamente un escaneo en busca de malware.

b. Conexiones Wi-Fi

Los Smartphone son cada vez más susceptibles a los ataques a través de WiFi, sumando a estos los ataques a través de aplicaciones que permiten acceder más fácilmente como lo son correo electrónico y las aplicaciones de redes sociales entre otros.

c. SMS

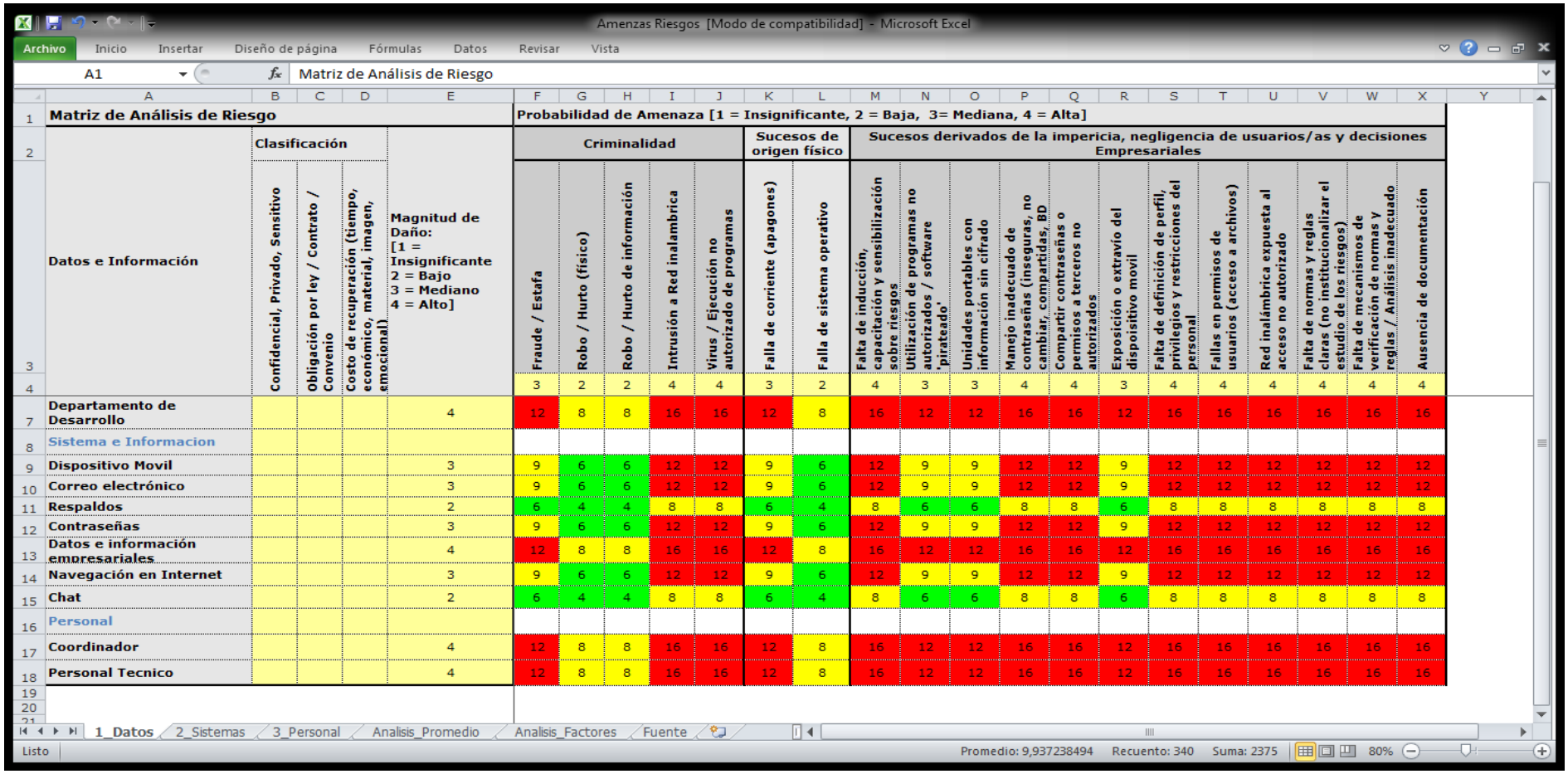
Hay que tener en cuenta que la mayoría de las infecciones reportadas se deben a troyanos SMS que envían mensajes a números de pago, a menudo a un costo irrecuperable para el usuario o empresa.

d. Perdida y el robo del Smartphone

Uno de los principales problemas es la perdida de los dispositivos estos se da porque bien fueron robados o perdidos por lo que es importante localizar, bloquear y borrar la información en el contenida.

Por ello es importante que los empresarios tengan conocimiento de los crecientes riesgos a los que están asociados el personal con la comodidad de tener internet en la palma de sus manos.

4.2.7. Riesgos obtenidos según análisis matriz



Amenzas Riesgos [Modo de compatibilidad] - Microsoft Excel

Archivo | Inicio | Insertar | Diseño de página | Fórmulas | Datos | Revisar | Vista

A1 | Matriz de Análisis de Riesgo

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																		
	Clasificación				Criminalidad					Sucesos de origen físico		Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones Empresariales											
Datos e Información	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información	Intrusión a Red inalambrica	Virus / Ejecución no autorizado de programas	Falla de corriente (apagones)	Falla de sistema operativo	Falta de inducción, capacitación y sensibilización sobre riesgos	Utilización de programas no autorizados / software 'pirateado'	Unidades portables con información sin cifrado	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD	Compartir contraseñas o permisos a terceros no autorizados	Exposición o extravío del dispositivo movil	Falta de definición de perfil, privilegios y restricciones del personal	Fallas en permisos de usuarios (acceso a archivos)	Red inalámbrica expuesta al acceso no autorizado	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado	Ausencia de documentación
					3	2	2	4	4	3	2	4	3	3	4	4	3	4	4	4	4	4	4
Departamento de Desarrollo				4	12	8	8	16	16	12	8	16	12	12	16	16	12	16	16	16	16	16	16
Sistema e Informacion																							
Dispositivo Movil				3	9	6	6	12	12	9	6	12	9	9	12	12	9	12	12	12	12	12	12
Correo electrónico				3	9	6	6	12	12	9	6	12	9	9	12	12	9	12	12	12	12	12	12
Respaldos				2	6	4	4	8	8	6	4	8	6	6	8	8	6	8	8	8	8	8	8
Contraseñas				3	9	6	6	12	12	9	6	12	9	9	12	12	9	12	12	12	12	12	12
Datos e información empresariales				4	12	8	8	16	16	12	8	16	12	12	16	16	12	16	16	16	16	16	16
Navegación en Internet				3	9	6	6	12	12	9	6	12	9	9	12	12	9	12	12	12	12	12	12
Chat				2	6	4	4	8	8	6	4	8	6	6	8	8	6	8	8	8	8	8	8
Personal																							
Coordinador				4	12	8	8	16	16	12	8	16	12	12	16	16	12	16	16	16	16	16	16
Personal Tecnico				4	12	8	8	16	16	12	8	16	12	12	16	16	12	16	16	16	16	16	16

1_Datos | 2_Sistemas | 3_Personal | Analisis_Promedio | Analisis_Factores | Fuente

Listo | Promedio: 9,937238494 | Recuento: 340 | Suma: 2375 | 80%

4.2.8. Riesgos de seguridad en Smartphone no controlados dentro de la Empresa

Las empresas en la actualidad no se percatan de los riesgos a que están expuestos en el uso de Smartphone dentro de las empresas ya que estos no son utilizados solo para su uso personal sino también profesional, la mayoría del personal usa estos dispositivos sin que hayan pasado por las manos del departamento de TIC de la empresa, por consiguiente esto presenta un gran riesgo en la seguridad de la información empresarial.

Si bien hoy en día el personal dedicado a la seguridad pone énfasis en la protección de la información almacenada en computadoras portátiles y unidades de almacenamiento removible. Esto no ocurre en la seguridad de los dispositivos móviles por ser un fenómeno reciente por lo que muchas empresas no parecen estar preparadas para este tipo de riesgo.

4.2.9. Soluciones de riesgo en seguridades de información dentro de la empresa

- Las empresas son las responsables de informar al personal las políticas sobre el uso de teléfono inteligentes personales, si van a proveer el uso del mismo dentro de la empresa, deberán exponer sus reglas de uso, así como exponer las penalizaciones que tendrán por su incumplimiento.
- En el caso de permitir el uso de Smartphone personales, el personal deberán comunicar al departamento de TIC, ellos serán los encargados de revisar el equipo para instalar el software necesario como por ejemplo un VPN con las medidas de seguridad apropiadas, instalar programas de

encriptación de datos, dando así un visto bueno para que puedan acceder a la información de la empresa.

- Los desarrolladores de los sistemas de la empresa deberán estar también preparados para filtra el trafico entrante, permitiendo el paso solo a los Smartphone validados por el departamento de seguridad e impidiendo aquellos que no lo estén.
- Se tendrá que instalar en los dispositivos certificado electrónicos que los identifique y autentifique dentro de la red empresarial, esto ayudara a gestionar la identidad y los privilegios de cada usuario y aplicaciones móviles.
- Otro factor importante sería el hecho de que los fabricantes de dispositivos móviles asuman un mayor protagonismo, diseñando productos teniendo en cuenta la importancia de la seguridad de la información y no nada más como simple electrónica de consumo.

4.2.10. Normas para prevención de riesgos en el uso de información dentro de las empresas.

- Los directivos deberán tener una atención especial en la redacción de las normas que deberán cumplir el personal, ya que estas no deberán ser únicamente para dispositivos de propiedad de la empresa si no los de propiedad del empleado también, para evitar conflictos futuros ya que el personal tiene que estar consístete que en el mismo se alojan datos de la empresa como clientes, proveedores e información crítica de la empresa.
- Estas normas deberán ser aceptadas por el personal de la empresa antes de la instalación en el dispositivo móvil.

- Una de las obligaciones del personal será el no modificar los parámetros de seguridad, el mantenimiento y actualización del sistema operativo y de las aplicaciones.
- Entra la normas de uso se deberán alertar al personal sobre los posibles ataques a la información que puede afectar a los datos de la empresa. Por lo tanto el personal tendrá la obligación de extremar la precaución en la descarga de aplicaciones para impedir la entrada de malware que pueda vulnerar la seguridad del dispositivo en sus cuatro capas (Aplicaciones, Hardware, Red y Sistema Operativo)
- El personal deberá tener un extremado cuidado del dispositivo ya que estos pueden ser utilizados por familiares, hijos, amigos siendo muy probable la navegación en internet con criterios de prudencia muy distintos a los del usuario principal, lo cual tendrá sus consecuencias en materia de cookies y publicidad sin ningún tipo de seguridad.

4.3. Determinar políticas de seguridad empresarial en el uso de Smartphone.

4.3.1. Sanciones previstas por incumplimiento

El incumplimiento de la disposición establecida en las políticas de seguridad de la empresa deberá tener como resultado la aplicación de sanciones, conforme a la magnitud y característica del aspecto no cumplido

4.3.2. Departamento de seguridad de la Información

- Deberá revisar y proponer al gerente y altos directivos a su consideración y posterior aprobación las políticas de seguridad de la información y las funciones generales en materia de seguridad de la información que fuera conveniente y apropiado para la empresa.
- Monitoreara cambios significativos en los riesgos que afecten los recursos de la información de la empresa frente a posibles amenazas, sean estas internas o externas.
- Evaluará y coordina la implementación de controles específicos de seguridad de la información.
- Promover la difusión y apoyo de la seguridad de la información dentro de la empresa.

4.3.3. Políticas y reglas de control de acceso.

Con el objetivo de impedir el acceso no autorizado a la información se implementaran procedimientos normales para controlar la asignación de derechos de acceso a los datos y servicios de información.

a. **Registro de usuarios:** Definir un registro de usuarios para otorgar o revocar el acceso.
b. **Administración de privilegios:** Se limitara y controlara la asignación y uso de privilegios.
c. **Administración de contraseñas de usuario:** se controlara a través de un proceso de administración formal.
d. **Administración de contraseñas críticas:** usuarios con actividades criticas como instalación de plataformas p sistemas, software, etc. estos necesitan mayor nivel de complejidad que el habitual

4.3.4. Políticas aplicables para la gestión de los recursos en la Empresa.

- El personal deberá seguir buenas prácticas de seguridad en la selección y uso de contraseñas, deberán cumplir las directivas que se impartan a tal efecto.
- Restricción del acceso a sectores de la empresa los mismos que contengan información sensible.
- No todos los recursos deben de estar accesibles mediante la utilización de estos dispositivos móviles.

- Tendrán que separar la red Wi-Fi que utilizan los Smartphone, de la red que utiliza la empresa, así se evitara que exista un acceso indebido a la red de empresarial.
- Tendrán que cifrar la conexión que utilizan los dispositivos móviles.
- Si las empresas no cuentan con políticas de seguridad es necesario que estas se establezcan conjuntamente con el departamento de TI.

4.3.5. Políticas aplicables para el personal de la Empresa en el uso de los Smartphone en las Empresas.

Es de vital importancia que las empresas creen políticas de seguridad con el objetivo de que el personal tome decisiones adecuadas sobre su forma de proceder en el uso de estos dispositivos personales dentro de la empresa.

A continuación se detalla algunas políticas que las empresas podrían aplicar:

- El personal no podrá compartir la información que contenga en su Smartphone con personal no autorizadas.
- Tendrán que utilizar los Smartphone solo con fines laborales, no podrán compartir la información con terceras personas ajenas a la empresa.
- La información de la empresa que contenga los Smartphone serán absolutamente confidencial.
- Deberá respetarse la normativa de propiedad intelectual e industrial.
- El personal de la empresa deberá capacitarse con el departamento de TI sobre los mecanismos para el ingreso seguro a la información a través del uso de los teléfonos inteligentes.

Una vez revisado las políticas aplicables en el uso de dispositivos El personal deberá firmar el acuerdo de la política de seguridad de la empresa, con esto se confirma que el personal entiende y acepta acatar las políticas establecida en el mismo comprometiéndose a cumplir las normativas de seguridad definidas por la empresa.

4.3.6. Normas aplicables en cuanto al uso de información a través de los Smartphone.

La redacción de la normas deben merecer una espacial atención ya que en algunos casos el personal tiene conocimiento de las normas referidas a dispositivos que son propiedad de la empresa pero desconocen las normas aplicadas para teléfonos inteligentes de su propiedad ya que a pesar de ser un dispositivo propio, en este se puede alojar datos personales de clientes, proveedores e información crítica de la empresa.

Las normas aplicables al personal serian:

- El personal de la empresa no podrá modificar los parámetros de seguridad.
- No podrá realizar actualización del sistema operativo y aplicaciones,
- Tendrá que realizar copias de seguridad.
- El personal de la empresa tendrá la extremada precaución en las descargas de aplicaciones para así impedir la entrada de malware que vulneren la seguridad del Smartphone.

Las normas establecidas deberán ser aceptadas por el personal antes de la instalación de las aplicaciones empresariales en el dispositivo de uso personal.

Se sancionara administrativamente al personal que viole lo dispuesto en la presente política de seguridad conforme a lo dispuesto por las normas de la empresa, en caso de corresponder, se realizara a las acciones correspondientes ante el o los organismos pertinentes.

4.3.7. Plan de Capacitación

PROGRAMA DE CAPACITACIÓN DE SEGURIDAD DE LA INFORMACION EN LOS DISPOSITIVOS MOVILES SMARTPHONE

a. Objetivo

Reducir el nivel de riesgo relacionado con la seguridad de la información de las empresas en las distintas actividades y tareas analizadas en la matriz de riesgos.

b. Recursos

Para el desarrollo del programa se cuentan con los siguientes recursos:

- **Recurso humano:**

  Srta. Dayana Cárdenas Vásquez

- **Recursos materiales, tecnológicos e infraestructura:**

  Salas de capacitación, equipadas con: Sillas y mesas, Equipos de proyección multimedia, Computadora portátil, Fotocopiadora, Impresora a color, Material de escritorio, e Internet, todo esto bajo la autorización del gerente de la empresa Enlace Digital Cía. Ltda.

c. Documentación

Como material de consulta y marco de orientación se cuenta con la siguiente documentación:

- Matriz de evaluación de riegos
- Políticas, normas y reglas aplicables a la Seguridad de la información
- Manuales, procedimientos e instructivos del Sistema de Gestión de Seguridad
- Crípticos de información útil referente a las seguridades

d. Control de ejecución

El control de este plan de plan de capacitación será realizado por la gerencia de la empresa.

CONCLUSIONES

- Tanto las empresas como el personal necesitan ser conscientes de los crecientes riesgos asociados con la comodidad de tener Internet en la palma de sus manos. Los Smartphone esta expuestos a una variedad de ataques, desde los que provocan que la batería se desgaste, hasta los que pueden dejar al Smartphone sin servicio, las vulnerabilidades que estos dispositivos móviles Smartphone poseen son: virus, spam, contagio de PC a portátil, etc.

- Es por ello que las Empresas deben tomar conciencia de las falencias de seguridad a la que están expuesta la información en el uso de la información atravesó de los dispositivos móviles Smartphone, deberán tener establecidas políticas y normas que el personal deberá cumplir a cabalidad bajo las restricciones planteadas en el mismo.

RECOMENDACIONES

Las empresas con el fin de protegerse contra las crecientes amenazas para dispositivos móviles, deberán se consistentes de lo siguiente:

Referente al personal:

- El personal deberá instalar en el dispositivo una solución antimalware para protegerlo contra las aplicaciones maliciosas.
- Tendrán que usar en el dispositivo un firewall personal para proteger las interfaces del dispositivo.
- Se requerirá la utilización de una contraseña robusta de protección para el acceso al dispositivo.
- Deberán Implementar software anti-spam para proteger contra comunicaciones de voz y de SMS / MMS.

Referente a las empresas:

- Emplear en el dispositivo anti-malware para protegerse contra aplicaciones maliciosas
- Centralizar el bloqueo remoto, limpieza, copias de seguridad y restaurar las instalaciones para los dispositivos perdidos o robados.
- Aplicar totalmente las políticas de seguridad, tales como ordenar el uso de fuertes contraseñas y Pines.
- Aprovechar las herramientas que ayudan a monitorear la actividad del dispositivo para la fuga de datos y el uso inadecuado.
- Centralizar la administración del dispositivo móvil para hacer cumplir e informar las políticas de seguridad.

BIBLIOGRAFÍA

1. Quiminet.Com (http://www.quiminet.com/articulos/que-es-un-smartphone-para-que-sirve-un-smartphone-60705.htm) Copiado el 18/11/2012.

2. Dispositions Movile Designed by Website Hosting Reviews (http://ingenieria-dispositivos-moviles.blogspot.com/2012_03_04_archive.html) Copiado el 18/11/2012.

3. Conatel(http://www.conatel.gob.ec/site_conatel/index.php?option=com_content&view=article&catid=48%3Anormas-del-sector&id=96%3Aley-especial-de-telecomunicaciones-reformada&Itemid=103&showall=1) Copiado el 17/11/2012.

4. Conatel (Http://www.supertel.gob.ec/index.php/table/derechos-de-los-usuarios/) Copiado el 17/11/2012.

5. ElTelegrafohttp://www.telegrafo.com.ec/index.php?option=com_zoo&task=item&item_id=5227&Itemid=11) Copiado el 09/11/2012.

6. Comunican S.A. elespectador.com http://www.elespectador.com/tecnologia/articulo-330538-dispositivos-moviles-son-claves-empresas copiado el 17/11/2012

7. Periódico el economista http://eleconomista.com.mx/tecnociencia/2012/05/08/dispositivos-moviles-vulneran-las-empresas copiado el 17/11/2012

8. Editorial borrmart http://www.borrmart.es/articulo_redseguridad.php?id=1489 copiado el 17/11/2012

9. Revista judicial http://www.derechoecuador.com/index.php?option=com_content&view=article&id=6662:formato-de-un-regalmento-interno-de-trabajo&catid=317:trabajo&Itemid=584 copiado el 17/11/2012

ANEXO1: BASE DEL ANTEPROYECTO

Carrera: Ingeniería de Sistemas

Estudiante: Digna Dayana Cárdenas Vásquez

Propuesta: "Análisis de seguridad de la información en los dispositivos móviles Smartphone**"**

1. ¿Cuál es el problema?

El acceso a la información en cualquier momento y lugar se ha envuelto hoy en día parte de nuestras acciones cotidianas. Forma parte de una arista más que las empresas de la ciudad de Cuenca necesita para mantenerse competitivas en el Mundo actual. Los dispositivos móviles (Smartphone) facilitan esta tarea en combinación con las tecnologías de conectividad emergente y tradicional (GPRS, EDGE, 3G 802,11, bluetooth y otra).

A partir de estas tecnologías, alguna de las funcionalidades de las empresas se extiende fuera de los límites, permitiendo al personal interactuar en donde quiera que se encuentren como por ejemplo:

- Acceso al correo de la empresa
- Acceso a los aplicativos de la empresa
- Sincronización de calendarios
- Sincronización de contactos que posee la empresa
- Almacenamiento y edición de documentos

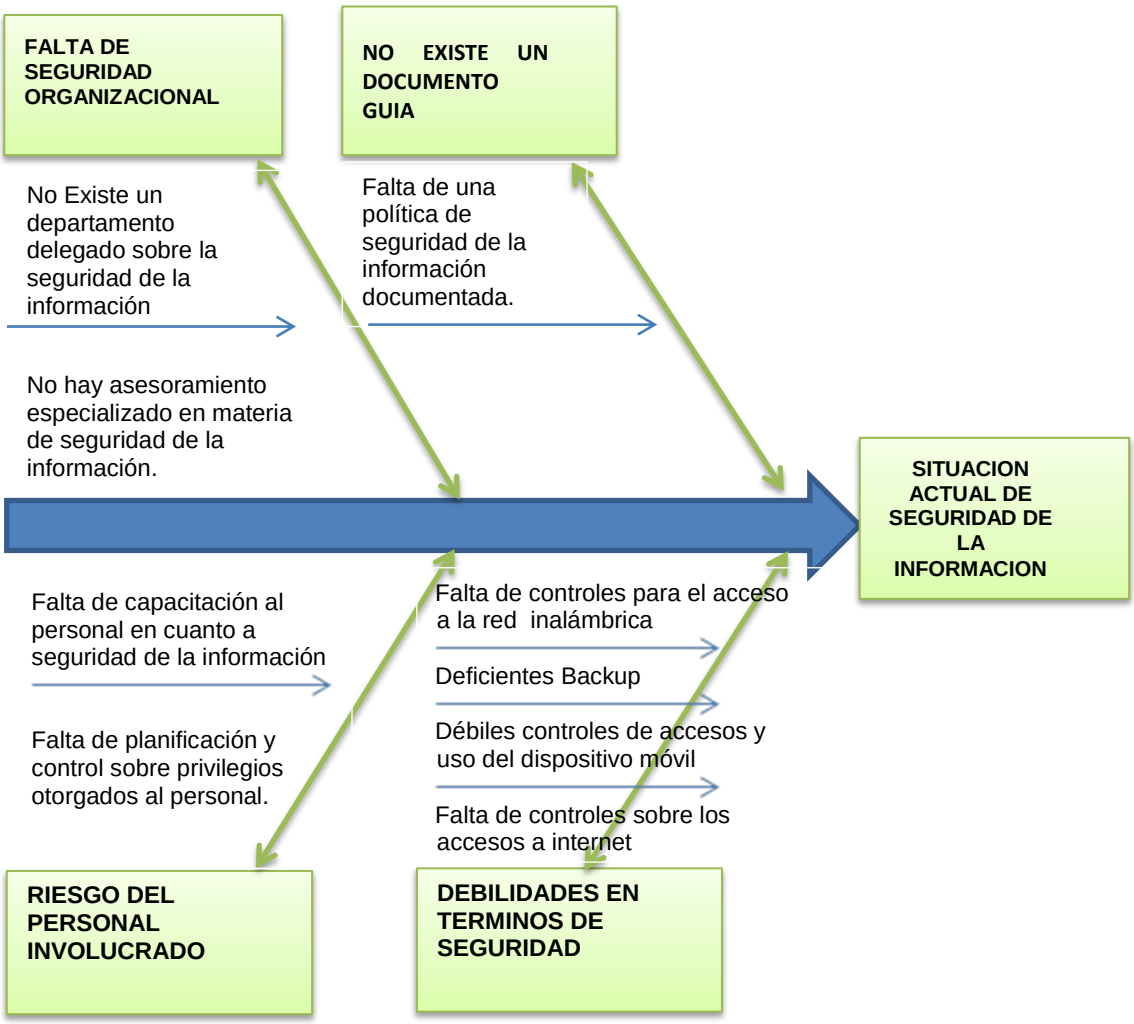
Los Smartphone, han ampliado las funciones de las PDA (Personal Digital Assistance) permitiendo utilizar dichos dispositivos tanto para fines personales como empresariales, y en base a ello entonces, dos frentes con diferentes tipos de problemáticas:

Problema I: En implementaciones empresariales, la aplicación de políticas de seguridad apropiadas, al igual que en una estación de trabajo, se plantea la misma pregunta:

- Como evito que el personal use el dispositivo con fines no relacionados con la empresa.

Problema II: por lo general, el personal, casi siempre de alta jerarquía, deciden, sin el más mínimo análisis, incorporar estos dispositivos a las redes de la empresa o bien incorporar información sensible en las memorias de almacenamiento de estos dispositivos. Si bien no es novedad que los dispositivos móviles ya están ocupando un espacio en los entornos empresariales, preguntas como las siguientes rondan:

- Se han evaluado los riesgos que estas tecnologías pueden introducir en los modelos de seguridad de mi empresa.
- Cuáles son los riesgos más representativos en el uso de estas tecnologías.
- Como puedo aplicar políticas de seguridad empresarial a dispositivos de uso personal y con información privada dentro.
- Si monitoreo el uso de estas tecnologías, estoy invadiendo la privacidad.



2. ¿Por qué es importante investigar sobre el tema?

Si bien hoy en día la mayoría entiende la necesidad de implementar y mantener políticas de seguridad acorde a las buenas practicas, muchas veces estas dejan fuera a las nuevas tecnologías y sus diferentes aplicaciones en la empresa. Es por esto que debe existir una norma de seguridad que haga referencia exclusivamente a la utilización de dispositivos móviles Smartphone, que cuente con el apoyo de la alta dirección y contenga entre sus objetivos:

- Proteger los datos sensibles de la empresa.
- Evitar que sean causa dela infección y distribución de código malicioso dentro de la empresa.

- Prevenir que sean estos dispositivos el origen de accesos no autorizados a las redes de la empresa.

Una de las características que incorporan la mayoría de los Smartphone de hoy en día es que son capaces de ejecutar programas y aplicaciones que añaden funcionalidad al aparato además de permitir la descarga directa de diferentes tipos de información, ficheros (Habitualmente multimedia o informáticos).

3. ¿Qué se conoce al respecto hasta el momento, dentro y fuera del país?

No hace muchos años los teléfonos móviles se encontraban aislados de muchos riesgos de seguridad al no estar interconectados con la Red. Pero actualmente, la inmensa mayoría incluye mecanismos para que puedan conectarse y descargar contenido de Internet, leer el correo electrónico, etc., y por tanto, enfrentarse a las mismas amenazas de seguridad que los equipos. Es por esto que, se hace necesario un análisis de las prestaciones que incorporan actualmente los dispositivos móviles y cómo las aprovecha el personal. También, cómo afectan estas prestaciones en los hábitos del personal en Cuestión de seguridad.

Links:

Instituto nacional de las tecnologías de la comunicación "Estudio sobre la situación de seguridad y buenas prácticas en dispositivos móviles y redes inalámbricas" tomado de: http://www.inteco.es/Seguridad/Observatorio/Estudios/estudio_redeshttp://www.red.es/redes/sites/default/files/estudio_moviles_3c11.pdf

Articulo diario la nación "La seguridad de los dispositivos móviles" Tomado de:http://www.red.es/redes/sites/default/files/estudio_moviles_3c11.pdf

4. ¿Por qué lo va hacer?

La utilización de Smartphone con fines empresariales incrementa de manera muy favorable la productividad pero puede transformarse en una nueva vía de ataque si no se implementa los controles adecuados. Lo mismo que sucede con toda nueva tecnología.

Antes de decidir incorporar o no estas tecnologías, se debe analizar los riesgos que pueden introducir en nuestra empresa de manera directa e incluso de manera indirecta. Se debe analizar cómo pueden impactar en el modelo actual de seguridad de la empresa.

No hay peor incidente de seguridad que aquel que ocurre y no nos enteramos, pero más frustrante es aquel que ocurre, nos enteramos pero no podemos determinar por donde vino.

5. ¿Cómo lo va a realizar?

Para la obtención de la documentación respecto a detalles de seguridades de Smartphone se realizará una investigación bibliográfica. Para la recolección de datos y realizar un sondeo del conocimiento que tiene las personas respecto al tema se procederá a efectuar encuestas y entrevistas.

6. ¿Cuáles son los resultados esperados?

Con el desarrollo de este análisis se pretende dar a conocer a las personas las seguridades de la información en cuanto al uso de Smartphone las protecciones y control de accesos al mismo. Así también se pretende que el lector tenga una guía de las seguridades de los dispositivos móviles que puede implementar y que mejor se adapte a sus necesidades.

7. ¿Cómo va a transferir y difundir los resultados?

Se realizará una publicación web en los sitios más utilizados para investigación y en bibliotecas digitales de universidades regionales.

8. ¿Qué efectos e impactos podría tener las nuevas tecnologías o los nuevos conocimientos en el grupo objetivo?

El impacto será Institucional y económico. Institucionalmente se tendrá un apoyo para la toma de decisiones al momento de implementar seguridades en los dispositivos en las empresas; económicamente ayudará a conocer precios y así estimar gastos.

ANEXO 2: ENCUESTAS

ENCUESTAS REALIZADA AL PERSONAL DE LAS EMPRESAS EN CIUDAD DE CUENCA

OBJETIVO: Obtener información directa del personal que laboran en las empresas en la Ciudad de Cuenca sobre el uso de los Smartphone.

ENCARGADO DE LA ENCUESTA: Dayana Cárdenas

I. SOLICITUD DE COLABORACION

Nos dirigimos a ustedes para solicitar su colaboración en el sentido de responder las preguntas de cuestionario, la información que usted provee es anónima y se maneja de forma eminentemente confidencial, solamente para los fines de esta investigación.

Agradezco su colaboración

II. DATOS DE LA ENCUESTA

1.- Sexo: M ☐ F ☐

2.- ¿Dispone de Dispositivos Móviles?

Si ☐ No ☐

3.- ¿Disponen de un Smartphone?

Si ☐ No ☐

4.- ¿Qué tipo de conexiones son las que más utiliza en su Smartphone?

Bluetooth ☐ Conexión 3G/GPRS ☐ Wi-Fi ☐

5.- ¿Habito de uso del Bluetooth en Smartphone?

- ☐ Lo enciende cuando lo necesita
- ☐ No utiliza y lo tiene apagado
- ☐ No utiliza y desconoce el estado
- ☐ Siempre encendido y visible
- ☐ Siempre encendido y oculto

6.- ¿Accede a su correo desde su Smartphone?

Si ☐ No ☐

7.- ¿Descarga programas o aplicaciones desde su Smartphone?

Si ☐ No ☐

8.- ¿Qué medidas de seguridad utiliza o tiene instaladas en su Smartphone?

- ☐ Pin para encender el teléfono
- ☐ Copia de seguridad
- ☐ Respaldo de número de serie (IMEI)
- ☐ Contraseña tras inactividad
- ☐ Antivirus

9.- ¿Qué incidencia de seguridad ha tenido en el uso de Smartphone?

- ☐ Ninguna incidencia
- ☐ Extravió
- ☐ Robo
- ☐ Fraude
- ☐ Virus Malware

Fecha: _____

Empresa donde se realizó la encuesta: _____

ANEXO 3: GLOSARIO DE TERMINOS

BLUETOOTH:

Es una tecnología que permite conectar dispositivos electrónicos entre sí de forma inalámbrica, o sea, sin cables (wireless). Por lo tanto pueden conectarse computadoras de escritorio o portátiles, celulares, PDAs (entre otros dispositivos) entre sí.

Wi-Fi:

Es una marca y también la sigla utilizada por la compañía que la creo para referirse a una tecnología de redes inalámbricas. Consiste en estándares para redes que no requieren de cables, y que funcionan en base a ciertos protocolos previamente establecidos.

PCMCIA:

(Siglas en inglés de Personal Computer Memory Card International Association: asociación internacional para tarjetas de memoria de PC), actualmente conocidas sobre todo como tarjetas PC o PC Card, se ha convertido en el estándar reconocido para uso en ordenadores portátiles.

PDA:

Un PDA (Personal Digital Assistant o Ayudante personal digital) es un dispositivo de pequeño tamaño que combina un ordenador, teléfono/fax, Internet y conexiones de red.

RIM:

Es una compañía canadiense de dispositivos inalámbricos más conocido como el

promotor del dispositivo de comunicación de mano BlackBerry. RIM desarrolla su propio software para sus dispositivos, usando C++, C y la tecnología Java. RIM también ha desarrollado y vendido componentes incorporados para datos inalámbricos.

MMS:

(Multimedia messaging system), un sistema para enviar mensajes multimedia entre teléfonos móviles.

SIM:

La Tarjeta SIM (son las siglas de Subscriber Identity Module (Módulo de Identificación del Suscriptor)), es una tarjeta que se utiliza en los teléfonos móviles en la que se almacena de forma segura la información del usuario del teléfono necesaria para identificarse en la red (clave de autenticación e identificación del área local). La tarjeta SIM también almacena datos del operador necesarios para el servicio de mensajes cortos y otros servicios.

SERVICIO DE APLICACIÓN J2ME:

J2ME propone un estándar de desarrollo para dispositivos móviles, permitiendo a los diferentes fabricantes (Motorola, Nokia, Alcatel, etc.) implementar la plataforma de ejecución (Máquina Virtual Java o JVM), o mismo utilizar la que gratuitamente brinda Sun MicroSystems para utilizar en sus dispositivos.

GPS:

GPS (Sistema de Posicionamiento Global). Es un sistema que sirve para determinar nuestra posición con coordenadas de Latitud, Longitud y Altura. Se basa en una constelación de 21 satélites que orbitan a la tierra a una

altura de 20200 Km, necesitando 11h58m para describir una órbita completa.

QWERTY:

Es la distribución de un teclado más común.

ARM:

Es una arquitectura de procesadores RISC de 32 bits desarrollada por ARM limited.

RISC:

Computadora con Conjunto de Instrucciones Reducido. Tipo de arquitecturas de computadoras que promueve conjuntos pequeños y simples de instrucciones que pueden tomar poco tiempo para ejecutarse.

ENCUESTAS REALIZADA AL PERSONAL DE LAS EMPRESAS EN CIUDAD DE CUENCA

OBJETIVO: Obtener información directa del personal que laboran en las empresas en la Ciudad de Cuenca sobre el uso de los Smartphone.

ENCARGADO DE LA ENCUESTA: Dayana Cárdenas

I. **SOLICITUD DE COLABORACION**

Nos dirigimos a ustedes para solicitar su colaboración en el sentido de responder las preguntas de cuestionario, la información que usted provee es anónima y se maneja de forma eminentemente confidencial, solamente para los fines de esta investigación.

Agradezco su colaboración

II. **DATOS DE LA ENCUESTA**

1.- Sexo: M ☐ F ☒

2.- ¿Dispone de Dispositivos Móviles?

Si ☑ No ☐

3.- ¿Disponen de un Smartphone?

Si ☑ No ☐

4.- ¿Qué tipo de conexiones son las que más utiliza en su Smartphone?

Bluetooth ☐ Conexión 3G/GPRS ☐ Wi-Fi ☒

5.- ¿Habito de uso del Bluetooth en Smartphone?

☐

- [ ] Lo enciende cuando lo necesita
- [ ] No utiliza y lo tiene apagado
- [x] No utiliza y desconoce el estado
- [ ] Siempre encendido y visible
- [ ] Siempre encendido y oculto

6.- ¿Accede a su correo desde su Smartphone?

Si [x] No [ ]

7.- ¿Descarga programas o aplicaciones desde su Smartphone?

Si [x] No [ ]

8.- ¿Qué medidas de seguridad utiliza o tiene instaladas en su Smartphone?

- [x] Pin para encender el teléfono
- [ ] Copia de seguridad
- [ ] Respaldo de número de serie (IMEI)
- [ ] Contraseña tras inactividad
- [ ] Antivirus

9.- ¿Qué incidencia de seguridad ha tenido en el uso de Smartphone?

- [x] Ninguna incidencia
- [ ] Extravió
- [ ] Robo
- [ ] Fraude
- [ ] Virus Malware

Fecha: Cuenca 17 de Noviembre del 2012

Empresa donde se realizó la encuesta: SysComp

ENCUESTAS REALIZADA AL PERSONAL DE LAS EMPRESAS EN CIUDAD DE CUENCA

OBJETIVO: Obtener información directa del personal que laboran en las empresas en la Ciudad de Cuenca sobre el uso de los Smartphone.

ENCARGADO DE LA ENCUESTA: Dayana Cárdenas

I. SOLICITUD DE COLABORACION

Nos dirigimos a ustedes para solicitar su colaboración en el sentido de responder las preguntas de cuestionario, la información que usted provee es anónima y se maneja de forma eminentemente confidencial, solamente para los fines de esta investigación.

Agradezco su colaboración

II. DATOS DE LA ENCUESTA

1.- Sexo: M ☐ F ☑

2.- ¿Dispone de Dispositivos Móviles?

Si ☑ No ☐

3.- ¿Disponen de un Smartphone?

Si ☑ No ☐

4.- ¿Qué tipo de conexiones son las que más utiliza en su Smartphone?

Bluetooth ☐ Conexión 3G/GPRS ☐ Wi-Fi ☑

5.- ¿Habito de uso del Bluetooth en Smartphone?

- [x] Lo enciende cuando lo necesita
- [ ] No utiliza y lo tiene apagado
- [ ] No utiliza y desconoce el estado
- [ ] Siempre encendido y visible
- [ ] Siempre encendido y oculto

6.- ¿Accede a su correo desde su Smartphone?

Si [x] No [ ]

7.- ¿Descarga programas o aplicaciones desde su Smartphone?

Si [x] No [ ]

8.- ¿Qué medidas de seguridad utiliza o tiene instaladas en su Smartphone?

- [ ] Pin para encender el teléfono
- [ ] Copia de seguridad
- [ ] Respaldo de número de serie (IMEI)
- [x] Contraseña tras inactividad
- [ ] Antivirus

9.- ¿Qué incidencia de seguridad ha tenido en el uso de Smartphone?

- [x] Ninguna incidencia
- [ ] Extravió
- [ ] Robo
- [ ] Fraude
- [ ] Virus Malware

Fecha: 18 DE NOVIEMBRE DEL 2012

Empresa donde se realizó la encuesta: MOTORALMOR CIA. LTDA.

Ing. Marcela Avila

ENCUESTAS REALIZADA AL PERSONAL DE LAS EMPRESAS EN CIUDAD DE CUENCA

OBJETIVO: Obtener información directa del personal que laboran en las empresas en la Ciudad de Cuenca sobre el uso de los Smartphone.

ENCARGADO DE LA ENCUESTA: Dayana Cárdenas

I. SOLICITUD DE COLABORACION

Nos dirigimos a ustedes para solicitar su colaboración en el sentido de responder las preguntas de cuestionario, la información que usted provee es anónima y se maneja de forma eminentemente confidencial, solamente para los fines de esta investigación.

Agradezco su colaboración

II. DATOS DE LA ENCUESTA

1.- Sexo: M ☑ F ☐

2.- ¿Dispone de Dispositivos Móviles?

Si ☑ No ☐

3.- ¿Disponen de un Smartphone?

Si ☑ No ☐

4.- ¿Qué tipo de conexiones son las que más utiliza en su Smartphone?

Bluetooth ☐ Conexión 3G/GPRS ☐ Wi-Fi ☑

5.- ¿Habito de uso del Bluetooth en Smartphone?

- [ ] Lo enciende cuando lo necesita
- [ ] No utiliza y lo tiene apagado
- [ ] No utiliza y desconoce el estado
- [ ] Siempre encendido y visible
- [x] Siempre encendido y oculto

6.- ¿Accede a su correo desde su Smartphone?

Si [x] No [ ]

7.- ¿Descarga programas o aplicaciones desde su Smartphone?

Si [x] No [ ]

8.- ¿Qué medidas de seguridad utiliza o tiene instaladas en su Smartphone?

- [ ] Pin para encender el teléfono
- [ ] Copia de seguridad
- [ ] Respaldo de número de serie (IMEI)
- [x] Contraseña tras inactividad
- [ ] Antivirus

9.- ¿Qué incidencia de seguridad ha tenido en el uso de Smartphone?

- [x] Ninguna incidencia
- [ ] Extravió
- [ ] Robo
- [ ] Fraude
- [ ] Virus Malware

Fecha: 8 noviembre del 2012

Empresa donde se realizó la encuesta: MotorAlmar Cía Ltda

Ing. Henry Loja

ENCUESTAS REALIZADA AL PERSONAL DE LAS EMPRESAS EN CIUDAD DE CUENCA

OBJETIVO: Obtener información directa del personal que laboran en las empresas en la Ciudad de Cuenca sobre el uso de los Smartphone.

ENCARGADO DE LA ENCUESTA: Dayana Cárdenas

I. SOLICITUD DE COLABORACION

Nos dirigimos a ustedes para solicitar su colaboración en el sentido de responder las preguntas de cuestionario, la información que usted provee es anónima y se maneja de forma eminentemente confidencial, solamente para los fines de esta investigación.

Agradezco su colaboración

II. DATOS DE LA ENCUESTA

1.- Sexo: M ☑ F ☐

2.- ¿Dispone de Dispositivos Móviles?

Si ☑ No ☐

3.- ¿Disponen de un Smartphone?

Si ☑ No ☐

4.- ¿Qué tipo de conexiones son las que más utiliza en su Smartphone?

Bluetooth ☐ Conexión 3G/GPRS ☐ Wi-Fi ☑

5.- ¿Habito de uso del Bluetooth en Smartphone?

- [ ] Lo enciende cuando lo necesita
- [ ] No utiliza y lo tiene apagado
- [ ] No utiliza y desconoce el estado
- [x] Siempre encendido y visible
- [ ] Siempre encendido y oculto

6.- ¿Accede a su correo desde su Smartphone?

Si [x] No [ ]

7.- ¿Descarga programas o aplicaciones desde su Smartphone?

Si [x] No [ ]

8.- ¿Qué medidas de seguridad utiliza o tiene instaladas en su Smartphone?

- [x] Pin para encender el teléfono
- [ ] Copia de seguridad
- [ ] Respaldo de número de serie (IMEI)
- [ ] Contraseña tras inactividad
- [ ] Antivirus

9.- ¿Qué incidencia de seguridad ha tenido en el uso de Smartphone?

- [ ] Ninguna incidencia
- [ ] Extravió
- [ ] Robo
- [ ] Fraude
- [x] Virus Malware

Fecha: 18 NOVIEMBRE DEL 2012

Empresa donde se realizó la encuesta: CONSTRUYICOR CIA. LTDA.

ING MANUEL VASQUEZ

ENCUESTAS REALIZADA AL PERSONAL DE LAS EMPRESAS EN CIUDAD DE CUENCA

OBJETIVO: Obtener información directa del personal que laboran en las empresas en la Ciudad de Cuenca sobre el uso de los Smartphone.

ENCARGADO DE LA ENCUESTA: Dayana Cárdenas

I. SOLICITUD DE COLABORACION

Nos dirigimos a ustedes para solicitar su colaboración en el sentido de responder las preguntas de cuestionario, la información que usted provee es anónima y se maneja de forma eminentemente confidencial, solamente para los fines de esta investigación.

Agradezco su colaboración

II. DATOS DE LA ENCUESTA

1.- Sexo: M ☑ F ☐

2.- ¿Dispone de Dispositivos Móviles?

Si ☑ No ☐

3.- ¿Disponen de un Smartphone?

Si ☑ No ☐

4.- ¿Qué tipo de conexiones son las que más utiliza en su Smartphone?

Bluetooth ☐ Conexión 3G/GPRS ☐ Wi-Fi ☑

5.- ¿Habito de uso del Bluetooth en Smartphone?

- [ ] Lo enciende cuando lo necesita
- [ ] No utiliza y lo tiene apagado
- [ ] No utiliza y desconoce el estado
- [x] Siempre encendido y visible
- [ ] Siempre encendido y oculto

6.- ¿Accede a su correo desde su Smartphone?

Si [x] No [ ]

7.- ¿Descarga programas o aplicaciones desde su Smartphone?

Si [x] No [ ]

8.- ¿Qué medidas de seguridad utiliza o tiene instaladas en su Smartphone?

- [ ] Pin para encender el teléfono
- [ ] Copia de seguridad
- [ ] Respaldo de número de serie (IMEI)
- [x] Contraseña tras inactividad
- [ ] Antivirus

9.- ¿Qué incidencia de seguridad ha tenido en el uso de Smartphone?

- [ ] Ninguna incidencia
- [ ] Extravió
- [ ] Robo
- [ ] Fraude
- [x] Virus Malware

Fecha: 18 noviembre del 2012

Empresa donde se realizó la encuesta: Enlace Digital Ons Ltda